Data Security & Privacy Committee Agenda

July 17, 2012 / 10:00 AM – 4 PM

Chicago Location:
James R. Thompson Center
100 W Randolph, suite 2-025
Chicago, IL 60601

Springfield Location:
Illinois State Library
Gwendolyn Brooks Building
300 W. Second St., Room 421
Springfield, IL 62701

Webinar Registration:
https://www1.gotomeeting.com/register/924229744

I. Roll Call

Mark Chudzinski welcomed the committee and took roll call:

Appointed Committee Members present in person: 1. Elissa Bassler 2. Jud DeLoss 3. Carl Gunter 4. Nicholas Panomitros 5. Harry Rhodes 6. William Spence	OHIT staff present: Mark Chudzinski; Krysta Heaney; Mary McGinnis; Laura Zaremba; Saro Loucks Invited Guests present: Marilyn Lamar; Steve Lawrence; David Miller; Colleen Connell; Bob Adams
Appointed Committee Members present electronically: 1. David Carvalho 2. David Holland 3. Tiefu Shen	Invited Guests present electronically: OHIT staff present electronically: Diego Estrella; Danny Kopelson; Cory Verblen
Appointed Committee Members absent: 1. Ron Isbell 2. Leah Bartelt 3. Jennifer Creasy 4. Timothy Zoph 5. Dr. Edward Mensah 6. Pat Merryweather	

II. Data Security and Privacy Committee Overview

Dr. Nicholas Panomitros, the committee's chairman, gave a committee overview, explained the need for policy recommendations, shared the committee's work plan and provided the day's agenda, as well as, procedure for public comment:

"To start us off, I will introduce the members of the Committee and highlight changes in its composition. Then I will speak to the history of the formation of both the ILHIE Authority and this Committee. Next, I will briefly explain the need for final privacy and security policy recommendations by the Committee. I would then like to share with you a proposed work plan and schedule for the Committee's deliberations on the issues presented, and entertain the Committee's comments and suggestions. Finally, I will run through Today's agenda that starts with ILHIE status reports and proceeds to testimony by 25 stakeholders divided into seven panels. The public is welcome to register for Public Comment at the door.

The ILHIE Authority Data Security and Privacy Committee comprises of fifteen members with personal knowledge of different areas of relevant expertise. Recently, Jim Anfield, the Senior Director of Strategic Relationships, Blue Cross Blue Shield of Illinois departed from the Committee and we would all like to thank him for his service and dedication.

The Illinois General Assembly created the ILHIE Authority in 2010 to develop and implement a state-wide health information exchange. The goal of the move was to enable health care professionals and providers throughout the state to exchange electronic PHI in a secure environment. The intention of the ILHIE was to improve patient care, the accuracy of prescriptions and orders and the reduction of health care costs.

The Data Security and Privacy Committee was created by the ILHIE Board at the close of 2011. I currently chair this Committee and have appointed the other 14 members. Any operating rules and procedures of this Committee must be adopted with my signature.

The Committee has two purposes: (1) Serve in advisory capacity to the Board on PHI data privacy and security policies and (2) Investigate and recommend ILHIE data privacy and security policies.

On February 8, 2012, the Committee held its first meeting where we discussed its formation, duties and governance. Furthermore, the Committee received a briefing on Illinois privacy and security laws along with privacy and security policy insight from Intersystems, the ILHIE technology provider. On March 29, 2012, the Committee invited five distinguished speakers to give testimony on privacy and security issues. The Committee held another meeting for invited testimony on May 3, 2012, which was part of the ILHIMA Annual meeting. There we had 8 speakers presenting testimony.

With the launch of the ILHIE near, the Committee has been given the assignment to develop recommendations for the adoption of privacy, security and consent management policies. Part of these recommendations will involve removing statutory barriers with the assistance of the Illinois General Assembly. Furthermore, the NhWHIN Governance RFI requests inputs from the states surrounding rules promulgated for the

national HIE. Thus, Illinois must solve the policy issues surrounding privacy and security on a state-level before offering input for the national HIE. The Committee's goal is to fulfill this task of providing Final Recommendations by September 19, 2012.

Today we will be taking testimony from more than two dozen stakeholders presenting on seven panels. There will be an overflow day on July 27 of this year that will also allow for the Office of Health Information Technology to provide briefings. Within two weeks of the overflow day, we will circulate the written testimony submissions. Next in early September, the Committee will conduct deliberations to discuss recommendations. Once the recommendations are drafted, they will be circulated to the Committee before the final report to the ILHIE Authority Board of Directors on September 19, 2012.

As I've mentioned earlier, the primary focus of today's meeting is elicit testimony from approximately twenty-five stakeholders taking part in each of the panels and the public. Key policy questions were identified and grouped into seven panels. After each presentation the members of the Committee will have the opportunity to seek further clarifications from the presenters. Before the testimony, there will be a status report given by OHIT on the ILHIE along with the four regional HIEs. Then we will hear from Panel 1 and 2 starting at 11AM before breaking for lunch at around 12:30PM. Then during the afternoon, starting at 1PM, the remaining five panels will present. The input of each member of the Committee, the stakeholders and the public is greatly valued and important

Finally, I just wanted to go over the procedure for public comment. Speakers will receive three minutes for testimony and there is a sign-up sheet outside with a description of the public comment process."

III. ILHIE Technical Infrastructure Overview

Laura Zaremba provided the group with an overview of the patient data privacy and Mark Chudzinski shared the security implications of HIE network:

"Thank you everyone, members of the committee, for being here today and on the webinar. We greatly value the work that you've put in so far and the time commitment that you've made to sort through these extraordinarily important issues. I also want to recognize the work of our general council: Mark Chudzinski, Krysta Heaney, and Mary McGinnis in putting together this particular committee hearing and subsequent testimony. I think, when it's all over, we will have elicited an extremely broad range of perspectives on this subject matter. And hopefully as I provide this brief update, with respect to the ILHIE network, we'll see how important it is for us to make recommendations for the broad privacy and security policy for the state to really support the continued implementation and usage of health information exchange services to benefit the healthcare delivery system and the patients of our state.

In today's presentation we would like to address two topics: I will discuss the overview of the architecture and implementation status of the ILHIE and Mark Chudzinski will provide an overview of the patient data privacy and security implications of HIE network.

As you are aware, the basic concept of a Health Information Exchange is to serve as the hub of an electronic network that facilitates the exchange of electronic patient health information among all of the participants in the health care system, including: regional and private HIE's, payers, hospitals, FQHC's, labs, pharmacy providers, large and small medical practices and multi-specialty groups.

Most medical treatment involves participants in geographically limited local and regional settings. But healthcare treatment is not necessarily confined to local and regional boundaries, and patient health records may need to travel beyond HIEs organized on a local basis. A state-level HIE would serve as an HIE of HIEs in Illinois, and in turn would be linked at the national level to state-level HIEs in other States.

An HIE enables the direct transmission of messages between providers. Such basic messaging functionality is also referred to as "point-to-point" or "directed" exchange.

A more robust HIE utilization of modern computing technologies enables the HIE to aggregate patient data from multiple sources and deliver the aggregated data in response to a data request from any connected user in the network.

In recent years, developments in Internet connectivity and other information technologies have led to an evolution in the concept of a federal hierarchical HIE network structure towards an Internet-based non-hierarchical network, in which any user can connect to any network at any level. Also of recent note are "private" HIE networks that are emerging: IDNs, ACOs, special purpose networks: labs, e-prescribing, EHR vendor-sponsored networks.

The ILHIE Development Strategy contemplates two initial phases: Phase 1: Direct Messaging (uni-directional; push) and Phase 2: Aggregated Data (bi-directional; query-response; pull). Focus: Transitions of care; Meaningful Use.

To implement Phase 1 Direct Messaging, ILHIE partnered with a commercial HISP to provide ILHIE Direct messaging service since Dec. 2011.

- *Similar to using e-mail*
- *Encrypted message transport to other Direct users*
- *Enrollment requires user identity verification*
- *Free through 2012*

ILHIE Direct Messaging is designed to address multiple use cases, and appears to be of particular utility when one or both parties to the data exchange are w/o EMR system (e.g., behavioral health services provider)

- *Phase One ILHIE Direct Progress to date:*
  610 signups, 87 active users
  Already exceeded Q2 registration goal
  End of year goal is 2000 signups

ILHIE Direct Messaging is a first step towards a user's progression to more robust exchange of structured data between EHR systems. ILHIE Direct Messaging does not enable the aggregation of patient PHI from multiple sources to more fully facilitate individual patient treatment and population health analysis.

In 2011 ILHIE retained a technology vendor, InterSystems Corporation, to provide the State of Illinois a robust "Software-As-A-Service" HIE solution.

- *Core components:*
  Master Patient Index/Record Locator Service
  Data aggregation engine
  Secure data transport/display
  Directories: Providers, Public Health Authorities
- *Initial ILHIE use cases:*
  1. Emergency room "pull" of aggregated PHI
  2. Clinical specialist referrals (using Provider Directory)
  3. Public health reporting via special node
  4. Provider incentive payment reporting

In test phase for bidirectional exchange
- *Testing Master Patient Index,*
- *Populating Master Provider Directory*
- *Will begin testing Public Health Node connectivity (late 2012)*

Current on-boarding pipeline
- *Chicago-based academic medical center*
- *Chicago-based FQHC*
- *Regional HIE in central Illinois*
- *Group of small hospitals in central/southern Illinois*

Estimate 2 to 6 months for GoLive
I will now turn over the remainder of the presentation to Mark Chudzinski."

Mark Chudzinski thanked Laura and continued with an overview of the patient data privacy and security implications of HIE network:

"Our health care ecosphere is complex. Successful treatment of a single patient involves multiple parties: multiple specialists; facilities and payers. Management of multiple parties and processes requires evaluation systems which measure and assess results. The sharing of clinical data among such parties is a key to successful health care.

Multiple parties contribute to the creation of patient data and multiple parties have interests in the use and sharing of such patient data, including: patients; providers; payers; public health authorities Accommodation of these multiple interest is an issue of policy and politics, less an issue of technology Importance of diverse stakeholder input to Authority Focal point of health care policy: the patient. Patients have concerns regarding potential uses of health care data, e.g. adverse insurance coverage determinations or employment decisions.

For addressing patient concerns regarding potential "misuse" of patient health data, two methods of legal protection are generally proposed: (1)"misuse" laws – restricting use of PHI, e.g. by insurance companies and employers and (2) "gatekeeper" laws – restricting initial release of data, principally by requiring patient consent for a release.

Most patient PHI privacy laws were fashioned prior to digital (EHR/HIE) revolution. They applied generally to point-to-point (unilateral directed exchange), usually involving a single point of release, a single data custodian, and a single recipient. Today's challenge is to consider how to take advantage of new HIT technologies while accommodating stakeholder interests affected by the new technologies. Today's aggregated PHI query-response (bilateral exchange) HIEs involve multiple points of data release, multiple data custodians, and multiple recipients – not all known to all parties at the time of the data release.

With regard to the operation of HIEs, one can suggest two key operational criteria. For HIE to effectively facilitate patient treatment: providers desire access to complete patient record; and data needs to be delivered on demand. With regard to HIE data flows: "misuse" laws – generally involve data use audits after data is released for use; while "gatekeeper" laws – generally require action by custodian of data; potentially impacts both "completeness" and "prompt delivery" of data for use.

"Gatekeeper" laws generally protect patient health data considered "highly confidential". In Illinois, as in most other states, the categories of specially-protected PHI include: mental health; psychotherapy notes, substance abuse, HIV/AIDS and genetic testing.

An example of a particularly challenging Illinois "gatekeeper" law is the one restricting disclosure of mental health data. The Illinois mental health confidentiality law requires patient consent with considerable specificity for release of data. It: Prohibits "blanket consent"; it prohibits "advance consent"; and it provides a durational limit on consent. The application of the Illinois mental health confidentiality law is unclear and arguably restricts any data aggregation query-response HIE to disclose mental health data without a new consent at the time of each data release. Future data recipients not known (at time of data creation) and date of future data release not known.

At this Committee's hearings on March 29, MetroChicago HIE brought to this Committee's attention the challenge it was facing because of the Illinois mental health confidentiality law and the intended deposit of clinical data by participating providers in a centralized data repository. As a result, MC-HIE has required of its HIE participants certain data filters: MC-HIE excludes from its data repository all mental health and substance abuse data; and requires its participating providers to secure all necessary consents for the depositing in the HIE of all "Highly Confidential data", namely HIV/AIDS and genetic testing data.

In order to implement the MC-HIE restrictions, we understand that the flow of patient records to MC-HIE is less robust that it otherwise could be. We understand that (1) all free text data is suppressed, for all patients; and (2) all patient records with any mental health data trigger are excluded. In conclusion, we note that the filtering of data by RHIO intermediaries has a potentially adverse effect upon ILHIE access to patient data.

Thank you for your attention, thank you also for your service on this committee and the opportunity to share with you these important issues and to receive your guidance. I'd also like to thank my OHIT staff colleagues for today's assistance, especially Krysta Heaney, Mary McGinnis and Saroni Lasker. I'd like to thank our summer legal interns who've participated in the papers that have been delivered to the committee,

especially Sara Nelson and John Saran. I'd like to thank the legal task force and its assisted attorneys, including Sonia Desai Bhagwakar and I'd like to thank the regional HIEs, Terry Jacobson in particular, for helping coordinate some of the testimony today."

IV. Regional HIE Technical Infrastructure Overviews

Marilyn Lamar thanked the committee and provided testimony (as an outside counsel) on behalf of Metropolitan Chicago Healthcare Council (MCHC) at the request of the Illinois Health Information Exchange Authority:

"Thank you everyone. My name is Marilyn Lamar. I'm here, unfortunately Terry Jacobson is not. But, I was with MetroChicago HIE, but Terry asked me to fill in for her. I'm outside counsel to MetroChicago HIE. MetroChicago has been working for over two years to launch the MetroChicago HIE. Due to time limitations we're going to try to describe a lot of what we're doing with respect to data and the privacy law impact in Illinois. But, of course, this is only a summary so I have to make the usual lawyer disclaimer: Not to bind MCHC.

In developing our approach we are working with a lot of different folks in the Metro Chicago area. We've been very fortunate to have a lot of input, not only from the state but from compliance officers, CIOs, attorneys and other participant representatives. I also note that we did do some focus group with patients and got their input at one point. I don't think any of that was particularly documented but that was done in a couple situations. The general approach that was adopted by MetroChicago HIE is opt-out. In other words, you have that very fundamental choice, as all of you are familiar with, whether it's opt- in or opt-out. The patients can decide whether none of their health information will be available to other participants, larger providers, through MetroChicago HIE – even for treatment.

The consensus was that clinical care would be improved more by opt-out approach, rather than an opt-in approach, because more data would be available to clinicians that are trying to treat those patients. We considered a lot of different things with respect with what to do about patients with conditions that require specific consent. We certainly didn't want to totally exclude them.

So what we came up with is a couple of categories. We said, well first, looking at all of Illinois and some relevant federal laws, we have to have a couple of exceptions, even with an opt-out approach. It was necessary to have exceptions to the general opt-out approach for two categories of data that require special treatment under state and/or federal law: (1) Highly Confidential PHI (HC PHI) which requires consent under Illinois law before disclosure even for treatment purposes and (2) Excluded PHI which requires authorization or consent under Illinois or federal law but the limited scope of use permitted after consent does not make it practical for access through MetroChicago HIE.

So with respect to the Highly Confidential PHI (HC PHI) we don't want it to be sent unless the participant, which is generally the provider, has obtained the required patient consent. And these are largely two areas: HIV/AIDS testing or diagnosis information and genetic testing information. We note in our agreement and for our working group that the scope is subject to change as laws change. And we hope some of

the efforts coming out of your committee and IL HIE Authority, in general, would be to get some legislative change, but for the moment this is what we think we have to do. And then some of our participants, we know, might be subject to additional laws that would make more data Highly Confidential PHI (HC PHI). For example, if we start linking to some state agencies that perhaps have even more onerous requirements on them as state agencies. So that it allows that flexibility.

The Excluded PHI, which is the other main category, we said 'Please don't send this to us. It should not be sent to MetroChicago HIE regardless of patient consent, due to limitations on scope'. As Mark identified, some of the very troublesome ones under the Illinois Mental Health and Developmental Disability Act under the Disability Confidentiality Act, Psychotherapy notes (per HIPAA Privacy Rule) and Alcohol and substance abuse treatment information subject to 42 CFR Part 2. So again, these definitions are subject to change as the laws change. But these are our two main categories. So we've said to participants per contract, 'Please don't send this to us. Use commercially reasonable efforts to screen it, filter it-Even if you got a patient's consent, we don't think you should be sending it'.

Participants responsible for first of all, looking at their records and determining if it includes this HC PHI and obtain patient consent or filter it out. Take appropriate action if consent later revoked, which is a whole other set of actions, which might be necessary if consent is revoked. Determine if patient record contains Excluded PHI and either filter it out or do not send patient records with Excluded PHI. And then, fundamentally, inform patient of right to opt-out of HIE data sharing at first visit and provide opt-in reversal form if requested later. And then, because this is happening, if you will, if you picture a hub and spokes approach, this is happening all along the edges of the wheel, before they send it to the hub. But tell us who's opted out and later opted back in, because we have to flip a switch at the hub in order to make those records unavailable.

Graph can be found on the PowerPoint:

Hopefully you've all had your coffee. Some of you really like these sorts of graphic representations. This is our attempt to come up to recording the patient consent and opt-out. This is how we look at this happening at a global level of Participant Registration Staff. So this is the staff, at the hospital, on the far left, would be capturing any necessary patient consent or revocation. That would go over to the right and to Participant Source System where it would be recording patient consent, or possibly revocation. And then, that stays at the participant- that stays at the hospital. But going back to that first column on the left, what they're going to do is capture this opt-in, opt-out reversal, etc., and tell MCHC so that shoots over all the way to the third column to record the patient opt-out or reversal and then MetroChicago would operationalize that. So for some of you this is helpful, others of us our eyes glaze over when we see these things, but it's a mixed media sort of approach.

Then we go to, okay, so how does the exchange work. So we have another column here. On the left, again, the Participant Source System would be sending this clinical message. You see at the bottom that black bar- That's stuff that gets excluded or filtered out. It's probably going through a Participant Interface Engine to administer

some of these filters and things they have to do. Then it goes over in the third column to MCHC and our portal gets stored. Then 5, at the bottom, under the MCHC row, is going to provide the patient data for viewing and then going back to the Participants on the far right, they request the data, that request goes to the HIE and then it comes back out to patient data view.

So having kind of gone into the weeds there, I think it's important to come back to some big issues. We have heard time and time again from clinicians and others, and even from patients, that we really want to maximize the amount of information in clinicians' hands. That is going to improve patient safety more than almost anything else- To not have this data excluded and having really complex, or what is referred to as granular restrictions are difficult to implement with the technology but they can also suppress more data than the patient requested. "Too many holes" is our nod to Mark Chudzinski, who I think has probably copyrighted the phrase "digital Swiss cheese". But it's memorable because too many holes discourage the clinicians from having coordination of care. And in this day of age, of accountable care organizations, and different reimbursement strategies, there are some financial elements to this as well. But overall, improving patient care is what we want to focus on. And we think we need more data rather than less.

So we can configure the patient data access to help identify the correct patient as well. Basically, what this means, is it would be wonderful if we could have a unique identifier for every patient. But, although that was part of HIPAA, one of the things that HHS was suppose to come up with by statute, every year gets blocked because a lot of privacy concerns have been voiced at the federal level. So we're in this world, where we have lots of people with the same or very similar names and all that confusion. We're trying to implement this in such a way, that for the most part, people will have to search with enough information. In other words, a participant that's seeking data will have to provide enough information to show that they really have this person in front of them, that they know the name, they know date of birth, they know address, a few things like that- So that they're not pulling up many more people and having sort of inadvertent access to more than they should. However, in some limited situations, we are setting the parameters a little more broadly to have more latitude in locating the right patient. And the obvious one there is in Emergency Room situations. So we'd love to get to a point with universal patient identifiers but it's just really difficult at this point. So that's where we are on that.

So you thought you were already in the weeds? So were going to go a little bit deeper into the weeds of opt-out, opt-in and patient consent here. Let's talk about some of the details we faced in putting this together. We struggled with this a lot, but finally concluded that the patient's opt-out decision at any one Participant will be effective for all of the patient's data in the MetroChicago HIE. So it's global, it's not limited to data. You know, gee, today I'm at my skin doctor, my dermatologist, and I want to exclude a piece of data that then is not available to my general practitioner, internist, whatever. We didn't think that that made sense, both from a technical perspective, but also back to a clinical perspective of wanting to have all of this there. So we decided to do it from a global perspective, again, with the patient in mind. And, in addition, the technology really does not easily permit a more granular level of opt-out.

And then, we get also into requiring participants, through our participation agreement to actually operationalize the opt-out. So we have contract requirements saying they have to offer the opt-out at first visit, first episode of care. They can offer it later if they want to, but it's not required. We did not time limit it, I understand there are some HIV/AIDS regulations that have just gone into place, so we may have to go back and look at some timing. But the opt-out does not expire at a specific date; the patient has to change it, if they want. Same thing with if they later revised and opted back in. An opt-out is only going to be effective on a "going forward" basis, but participants, obviously, if they had a patient in there and an opt-out had not been exercised for, let's say, six months, they've gotten lots of data from MetroChicago HIE, we've written this such, so that what they're keeping in their records is going to be, they're enabled to keep it, they don't have to go flush it out of their records just because a patient later opted out. So again, we are truly in the weeds on some of this stuff, but you guys probably will be to.

So if the patient later reverses it, so an earlier opt-out is no longer the case, again, it's going to be global. Then we came down to, well, what about the data in the gap period. So the patient opted out and now he's opted back in, what do we do about that data? How much data will the clinician be able to see? What we decided was that the clinician should be able to see the data, even from the period of opt-out. And, the important thing here is that we're disclosing this to the patients. So they know the consequences of opting back in. Something they thought they were trying to exclude will now become available if they opt back in.

As I've talked about with many of you, and we've struggled with, there's no so-called "break the glass" exception in Illinois that cuts across all statutes or anything. There are some little emergency exceptions in a few of the statutes, but they don't read the same way-So one of the goals, or policy recommendations might be to have a general emergency exception. This gets really confusing when you talk about HIEs in other states, because many of them do have strong emergency exceptions and we don't. So, again, I would recommend that perhaps for your consideration. We do disclose to patients, that if they have opted out, that there's not going to be emergency access, the information is not going to be there. And the excluded, highly confidential information, importantly, will not be there. And that goes to the policy issue as well, on the excluded PHI, even if someone were trying to get to it, it's just not going to be there, it would be filtered out of the HIE from the beginning.

A couple of special issues on the Excluded PHI, again, this is primarily records from alcohol / drug abuse treatment centers and mental health / developmental disability records. We've had all kinds of interesting issues in trying to work with participants about how the heck to filter this. For example, one hospital brought it to our attention that someone may come in through the Emergency Department, don't know what's wrong with them, but we later find out that this trauma they had was an attempted suicide or something where there's a mental health condition. So at first, the records, you just take them in because you don't know this is Excluded PHI and then it becomes apparent there is. So it gets difficult. Some participants already had systems in place from other states that were excluding based on primary or secondary ICD-9 codes. That may or may not be sufficient to really comply with law, but that's one approach

people are taking. If we exclude all patient records from psychiatric units – Is that too much excluded? You know, now we don't know important information that's potentially non psychiatric because people are sometimes in there for more than one thing. And then the medications, I think increasingly my perception as a law person is that so much more psychological/psychiatric treatment now is drug related rather than just, you know, therapy nodes, sessions. But those drugs are sometimes given for reasons other than mental health. I know someone on one of the workgroups was saying 'Yeah, I'm taking Lyrica, but it's because of pain, not depression, or whatever Lyrica is prescribed for'. So you are excluding too much if we really try to operationalize through a computer system the fact that somebody is on a drug that may be given for a psychiatric reason.

Additional concerns: Alcohol / substance abuse treatment centers really, I think, won't be able to send (publish) data to an HIE under current law. That's involving medications, but the data, if it's excluded, we can't get drug interactions which is a problem. The question arise: Whether we're having a new "digital divide" developing where these vulnerable patients that are in mental health or alcohol/substance abuse treatment centers really are not having their important data get into HIEs. They're not getting the benefit of the technological improvements of having the data available. And that strikes me as not a good result. Okay, we have talked a little bit, we haven't had anyone take us up on this yet, but these special treatment centers could participate to simply receive PHI. If they've got a patient who's having abdominal pains, and you wonder if it's appendicitis- Maybe they should be able to access the records not published to them but simply access and say 'Oh that person has had their appendix out already, don't have to worry about that particular thing. They wouldn't be sending or publishing so it's like half a loaf, but we've, we're willing to consider that.

A couple of other issues for filtering: It's really hard to figure out what to flag and filter. For example on the Genetic Testing statute our participants were quite perplexed that there was no easy list of what the heck to filter out. What is a genetic test? And again, I think things are just leap frogging with the science to have more and more genetic tests and to have to filter those out, it is difficult. Also, the text documents that Mark mentioned, some of our participants are trying to suppress all of them, it's not uniform, people are doing different things. But the simple word 'depression' if you tried to filter out for that word, you shouldn't be filtering out 'Depression of the skull' or 'No history of depression'. So, when you're thinking computers and its very literal-its difficult. So we had some fairly good-sized hospitals dealing with this so far. I think it's going to be really hard for small physician practices to deal with this as it goes forward.

So, in conclusion, we really appreciate this opportunity to present the testimony and to work with IL HIE and the Authority to find practical solutions. We are very focused on patient care and we also look forward to hearing testimony from others. I unfortunately have to leave fairly soon for a meeting, but if you have any questions, comments, whatever, at this time or later [recording unclear] MCHC reps here.

***Audience Member #1**: I was curious if you could tell us a little bit about how the providers are identifying excluded data? Going back to slide 10, there was a description of how the providers take the excluded data out. I was curious how your providers were*

doing that and how reliable they think those techniques are? Whether it causes them to, maybe take out too much data in some cases or even fail to participate in exchange?

***Marilyn Lamar**: Thank you. I will note that I'm the lawyer, not the technical person. But, my understanding is that they've had to custom fashion filters. And they've gone out of pocket with their EHR providers to try to develop filters. There isn't anything quick and commercial on the market, unfortunately. And they have had a lot of concerns about whether they're filtering out enough, whether they're filtering out too much. They have concerns about whether they're within the four corners of the law. And some of the patients aren't making it in there would be my guess. Because very few people are referred to horror stories but people coming in the fault able conditions some of which are psychiatric some of which are just regular parts of your body and serious issues. Those people I fear that the quality care that they're getting aren't as good.*

***Audience Member #2**: If you have to be statistics of what is the experience of patients decision making around opt out, they're given the opportunity to opt out- how many are opting out? How many are saying 'Yeah, sure, I think I want to be in the HIE'?*

***Marilyn Lamar**: We don't have any data yet, from Illinois. Anecdotally, from other sates, and in opt out we have many more participate than in opt in. Which you can kind of understand, you've already structured your system to be opt in, but you wouldn't get as many people. It's sort of a scarier consent. But I think also what's interesting is when we've gone and talked to some focus groups of patients, in this process, they all assume that everyone has this information anyway. It's amazing that they think all their providers already have this, and of course they don't.*

***Audience Member #3**: My question relates to the people who choose to opt out: When you filter it- are you continuing to collect information on individuals that opt back into your behavioral system, so their in there … The other question I had was about- are you planning on doing any statistics on what percentage of the people who choose to opt out, later choose to opt back in?*

***Marilyn Lamar**: As for the first question, it was a hotly discussed topic. However what we decided was: hospitals who want to, can go on sending data to the HIE, even though there's an opt out. In some instances, technically, it was the only way they could do it, from their systems perspective they couldn't filter out certain patients. And HIE, is MCHC's HIE, is responsible for flipping the switch, saying 'That's not accessible' and that is why we can, it flips back to being opt in, we do have all that data. And we will, of course, keep track, I'm sure it'll be obvious as to whose opted out and opted back in. We'll be able to keep those numbers, I suspect. We haven't discussed it, but I'm sure we'll do something like that.*

***Mark Chudzinki**: Dr.Shen in Springfiled, or any of the committee members on the webinar participation: Do you have any questions for Marilyn Lamar of MCHIE before she unfortunately needs to go to another engagement?*

***Tiefu Shen**: Yes, this is Tiefu Shen from Springfield, I do have a question. In addition to improving individual patients and improving patient safety, is improving public health and disease monitoring is also appropriate of this system? And if so, have you assessed the impact of patient opt out in some of the disease completeness and data quality?*

***Marilyn Lamar**: We would like to be linking to the State and Population Health. I think it's a future use case though, more than immediate. And also, there are some further issues there in terms of what we can or should be doing, as a private HIE. So I guess I kind of defer on that one, but we're very interested in population health issues. It's one of the issues we'd like to do. But the opt out, and I guess I should say to, is what I described as the use case opt out etc. is for other participants to pull the data and look at it for clinical care of the patient. There is another use case that MetroChicago HIE has that I think is lagging a little bit the first one, it's more clinical care. But we'll enable the participants to directly send information that's required to be reported to state agencies. And I'm not a technical person, so I'm not sure entirely where that stands in terms of interface with the state agencies. But in those cases, some of these things we've talked about as excluded, like the HIV/AIDS. Those are required to be reported. So there will be a separate database that doesn't have that stuff scrubbed out of it, as to those conditions that have to be reported. Because, certainly, right now, what I understand is it's very paper and fax driven and very mechanical to try to do that reporting of specific disease conditions for population health. So we will be trying to help people automate that with trying to avoid any overlap with the state.*

***Audience Member #4**: The question I have is in regards to behavioral; health for adolescences. Lets say at an early age, you know, they have behavioral problems. I heard you say in your presentation that when you become an adult your information because viewable. How would do you plan on handling that at an early age? Lets say, for example, they don't want it viewed as an adolescent, but when they become an adult and then they say, 'Yes, I want my record out there', does that part now part of the whole record? Are you seeing their adolescent record as well?*

***Marilyn Lamar**: All of the mental health records are being excluded right now, whether their children or whether their adults. We don't want our participants to send that to the HIE. So I think our participants are scrubbing that, filtering it, excluding it as much as possible. So it's simply not arising yet, because under current law, as Mark indicated, the Illinois mental health confidentiality statute is such that you can't have a blanket consent, or some sort of prior authorization. It has to be very in the moment and narrow. So from our perspective, you just can't do it through an HIE at present. So there really won't be any way for them to say, you know, those kinds of records aren't even subject to the opt in, opt out, they're totally excluded. I know it's like layers and layers, it truly is.*

***Audience Member #5**: But what is the policy with respect to the use of the data collected by the HIE for research safety identified data being shared for research?*

***Marilyn Lamar**: All of our participants were very concerned, rightfully so, about use for research. And so there were fairly long provisions in the participation agreement about not doing any research using the data without their consent. By the time you have truly de-identified it, it's not really good for research. We will be adopting a policy going through the advisory council and probably the board of MCHC to come up with some policies about this, because obviously there will be a lot of data here, and we're just starting to edge into that. But it was an issue that was a hot button for everybody that looked at this to sign on the participation agreement, to say what are you doing about research.*

***Audience Member #6**: I have a comment and a question. Have you considered having the mental health data by vaulting into the specific are of the Regional HIE, where you can have more stringent control? Our research has shown that there's a risk not only for the patients, but the other mental health residents in the behavioral health facilities. So for example, a patient from one facility is sent to another facility and their data is suppressed. They're placed in the general population with other behavioral health patients and they're unaware that this patient may have homicidal tendencies or something. Someone else gets injured. Would you consider- Have you considered providing mental health data, making it available to other mental health facilities only?*

***Marilyn Lamar**: Thank you. We don't think we're kind of steimet by the legal rules we have to operate under. We don't feel like we necessarily could do that under Illinois law, currently. You know, that may be one of the things that you all want to look at, in terms of committee work and public comment. But for MCHC, kind of getting going and starting this, we decided that the mental health stuff was too difficult because of no blanket consents, and things like that. I could see the state, I look at that very differently and probably should. I speak as a citizen and not as MCHC there, when I say you sure would want to know if other people in that institution had violent tendencies. That would be a good state health and safety regulation. But we didn't think that as a private, regional HIE, we could do that.*

***Audience Member #6**: When you talked about research and you talked about the extent to which the agreement with your participating hospitals sort of cover the issues of research: does that include using the data in a more aggregated fashion around public health assessment or for sort of understanding in the entire patient population that you have in the HIE, what's the percentage of people who have diabetes? And what's their racial and ethnic characteristics, and sort of mapping that. It's a little bit different from research and doesn't usually require sort of IRB approval and that sort of thing. Is that also under your sort of research restrictions right now?*

***Marilyn Lamar**: We have some broader rights to look at population health. We haven't started to yet, it's going to be something that I think has to be pursued to some policies. And the way we've constructed this is there's an advisory group that is made up of participants and some others who will give us a lot of good input. They've gotten us this*

far, in terms of making a lot of these choices. And then probably the full board of MCHC will weight in on this. But we are very interested in doing things with population health.

***Mark Chudzinski**: Thank you, Marilyn. If there are no more questions from the committee or those present, I'd like to now invite David Miller from Central Illinois HIE.*

David Miller presented to the committee his testimony on behalf of Central Illinois Health Information Exchange (CIHIE):

Thank you, Mark, and thank you to the committee for taking our testimony on all this today. We are very anxious to get the ILHIE Authority's guidance on how we're going to handle some of these things and clarify a lot of the concerns and a lot of the issues our participant have currently. So anyway we can help.

First of all let me introduce myself, I'm David Miller. I'm the technical lead for Central Illinois HIE. I've been with the HIE since its inception, since the planning phase. I have about 25 years experience in information technology and infrastructure management. I have experience in security administration and I have a master's in science information insurance from one of the Department of Homeland Security's certified institutions. So all of that means, while I probably don't know the answers, I know how scary the questions are. And we're anxious to move forward with that.

On the first slide that you saw there was a list of some of our [recording unclear] organizations. Some of you have probably heard that the first week of June former Anchor hospitals are actively collecting consent and collecting patient data. So we are actually live. We don't have clinicians in looking at the data yet, because we're of the opinion that until there's 60 to 90 days of data, its not worth our clinicians time, to take a look at it. We don't want to discourage does from using the system by having them go in and not find anything. So we're going to wait until the data goes up a little.

We expect OSF, St. Francis and the rest of the OSF system to come on board probably within the next 30 to 60 days. And we expect Advocate Brommen to be in within that time frame, probably a little bit sooner. So right now we've got Methodist, Decatur Memorial Hospital and St. Mary's in Decatur and St. Mary's in Springfield, IL. It's been very difficult for us to get all of this together because of their concerns regarding what they can share, and how they can share. Consequently as you will see throughout the rest of the presentation what we ended up doing is nowhere near, I think, what would be -it does not mean for an objective. [Recording unclear] It's a start but it is not as efficient.

Some of you have probably have seen this information before, just real briefly. This is a list of the, during the planning phase the state home rev that we perceive and we were very proud of the fact, as you see in that last paragraph, we have more than 200 people from organizations across 20 counties donating roughly 83 days per month, for 12 months of time, in terms of determining what it is that Central Illinois HIE should do for the stakeholders in Central Illinois. We've tried very, very much to stay with their vision and their interest and their concerns.

Those objectives, as they came out of that were to: improve care coordination,

decrease duplicate tests & services, reduce medical errors, provide better information to patients and improve overall health in community. And really what all of that boils down to is better care coordination all together. That's the central piece. Consequently, our focus initially was going to be, and is, to create what we call an Aggregate Community Record.

Our vision for that Aggregate Community Record was that it would include the items that you see there. And you will notice that we have planned 'x' to medication lists, transcribed reports, and medical history. We are unable to accept any of that data from any of our participants, at this time, because there's a possibility it could have behavioral health, it could have genetic testing and it could have any other sensitive areas that range. So, on the safe side we've excluded entirely, which means all we're really getting is labs, okay. I mean, it's helpful, its nice to know that somebody had a lab, it's nice to know that they had an x-ray, you know, at another facility. But it isn't the health history. And It's not going to save our patients from having repeat their health history every time they go in to see a physician. Which is one of the things that they really wanted, they wanted their data to be in and they wanted it to be permanent, so that they didn't have to continue in trying to remember all the details every single time, with everybody that they visit. We also recognized very early on the importance of direct messaging because of the fact that we will probably never be able to share behavioral health information. We hope its not, that there's some accommodation made, it certainly doesn't look like there will be. Except for point to point in a [recording unclear] of a range. But that is at least a method where the physicians at the hospitals or at the private practices can get information regarding their patients directly from the behavioral health providers, and as the MetroChicago pointed out, our Human Service Center, that is behavioral health. As expecting to use and view the medical records that are in the HIE, they will know when their patients are at the emergency room, they will know when they're visiting their primary care providers. And we believe that will help them track, follow and manage their patient care much better. So we'll see how that all plays out.

This is a very confusing diagram showing basically how the all charts system is organized. The green circle, which I know is really hard to read, is the system that we use to retrieve and store HL7 messages and we take individual data feeds from each of the participants and those feed into individually secured vaults. It's not technically separate databases and it's certainly not separate servers. But it is certainly segments of the database that are completely secured and walled off so that in effect all that the participant is doing is moving the data that's appropriate into a location where we can more easily retrieve it when it's ready to be disclosed. We do not consider that at that point it has been disclosed or released. It is ready to be disclosed or released but not disclosed or released. We'd certainly like to have a more definitive decision line whether or not that's and the same thing applies to the yellow over here, to our CCD exchange technology. The CCDs that are sent are walled off, so that again, if a participant has, and they are capable of exchanging CCDs then they'll actually be able to exchange them correctly with us and we can create a virtual health record for our HL7 side, which we call All Charts. Or we could create a virtual CCD for the HL7 data for our participants who are connected to out CMR.

What I touched on just a minute ago, the 'Data Collection versus Disclosure', we are capturing all of the opt-out data, and we're sequestering it, we're marking it and we're holding it. We're doing the same thing with sensitive information, where we can. We had several participants who decide they just didn't feel comfortable sending it in. But we rather that they send it in and we secure it, because if they don't send it in those particular encounters are lost. We're not backfilling dates, so every piece of history we don't get is a piece of history we won't have. It's better to have the data and have it secured and sequestered, we think, than to not have the information. So, if at some point in time, when the patient decides that their ready to share it or the legal environment is such, that we may be able to share it the day it is there, and it can be appropriate to share, appropriate controls. We are also, just like MetroChicago, using the opt out model, for the same reasons that way did. So we won't go into a whole lot more in detail. I will say that in our first three weeks in the end of June, we had 60,000 individual registered in the system and we had 8 opt-outs. So, it's not nearly a big of deal as you would've thought. That's, you know, that's one for every 10,000 roughly. We hope that that will continue. We think part of the reason why that is the case- and I'll touch on this again in a moment- it's only a clinical system. We are not allowing, at this point, secondary use of the data. And, in fact, because we don't actually store the aggregate record anywhere- that means every time we want to do like a report we actually have to query all the systems and aggregate the data. So it's not sitting somewhere all ready to go. It has to be, you know, pulled. That has its disadvantages, but the advantage, of course, is that all of that data is not sitting as a sweet honey pot for some hacker to go get, because it's all over the place. The data is distributed, it's a hybrid federated model. We are using a form of consent, which means that what our participants are doing is their modifying their notes of privacy practices and when the patient comes in for the first time, after they join the HIE- they all have a method of cracking this- they hand the person their notes of privacy practices along with a brochure. At least in most cases, in some cases they're not even handing them a brochure, they're just explaining it to them very quickly. In most cases they're handing them a brochure that explains that they're participating in the HIE, this is what it involves, and this is how you can opt-out if you'd like to. The registration people are not going through that conversation. Our participants were very much against that, and as we listened to their argument, we became very much against it as well, because the registration people are too busy to explain it well and they're not well versed in privacy or in issues that are really involved to advise a patient about what the real risks are. Consequently, this brochure has a form in it that they do fill out, they bring it back to the participating organization, to a contact person. That contact person either is, or knows who is, somebody who is well versed in privacy can discuss the issue, you know, with the patient. We have the capability being able to opt out all the data from a participant an entire encounter or just a result or document, we hope that, and this is the training we are giving the people who are doing this that they will be able to uncover what the real source of the concern is for the patient. And mark only what is really bothering them, if possible. We know for a fact that in all cases so far they opted out entire participant or organization. We do not have the capability of opting a person out from one participant for the whole HIE. That's a little bit different way then most people think about this. If

somebody visits, say, OSF St. Francis and opts out they aren't opted out from Methodist. If they decide they want to opt out later after the participants has joined they will have to visit each of the providers that they went to, we realize this is kind of both an education issue and also not super convenient for the patients, but it provides some flexibility too and that's how we're really trying to phrase it to the patients. Because they can choose not to share data from a particular specialist and everything else will be available so it makes it really easy for them to edit based on those decisions. We share the same concerns regarding break the glass and emergency access that the MetroChicago does, we're currently not going to allow it. We have another couple of additional issues. Because, as Mark pointed out in his presentation, this is one of those, you know, after the fact disclosure things, you can only really check it to make sure that somebody appropriately broke the glass, through an audit. The damage is done, the information is out there. Two of our participating organizations were not comfortable with that because they thought like if they were assuring their patients, they were opting them out, that their data should not be available anywhere under any circumstances, especially not where they didn't have any direct control over the provider or the employee that was looking at the data. So, we took that into consideration and agree with it. And then, on top of that, our vendor has shared with us that all of the EMR vendors they have integrated so far using CCD exchange and XPS, are unable to support break the glass in BPTC so that would, that meant for us that anybody who was, at least in the short term, going to be doing CCD exchange would be unable to facilitate breaking the glass, which would be an uneven situation where a certain hospital can do it, but another hospital can't do it. It's a problem with patient inception; it's also a problem in terms of the expectations of the patient. If they don't go to Methodist and Methodist isn't able to look at their data, in a case of emergency, we don't know what the ramifications of that would be. Since they were under the impression, probably from their other provider, that data would be available. So instead, again, because the way that we're handling patient consent, collecting it with a very human intervention, we're consulting with patients and advising them that if they opt out that information will not be available in a case of emergency. And we anticipate that there will probably be some people who will say, 'You know what, I really do kind of want it there'. So maybe, that's the deciding factor. If not, they understand the consequences that its really best. And so far, again, the opt out level has been so low, it's not really too much of a problem.

Regarding the secondary uses, I'm not an expert on this at all, because I'm not an informatics person, never really been involved in the occupation side, I'm an IT infrastructure guy. You know, I did servers and I did applications. So, I don't think I can truly appreciate all the nuances that are in this, but it seems to. It seems in discussing this around our age, that most of the reasons we secure the data have to do with sharing something embarrassing with somebody else. Sharing something with an employer that might adversely affect at work. Sharing something, you know, that might become available in a legal setting, and might adversely affect the judge. All of those things need to be centered around stuff outside of care delivery. So we really think that in the short term, until we can solve the issues with de-identification, and provide de-identified data perhaps on a case by case bases. And by staying with the clinical use only situation, that we can probably argue for sharing more of the data with greater level of

patient trust than if we don't. Now, that's a highly unpopular position with our parent organization, quality plus health. We understand that we're going to have all that data there, and ultimately advancing care is going to require that we are able to analyze and utilize the data to improve care, and especially improve care management. I just don't know that we're there yet, and I don't think we can afford to wait to do information exchange until we're ready to share it for secondary purposes. If we can go ahead and, at least, not wall that off, allow it for the future and continue to investigate it as an additional phase, at least from our perspective, highly adventitious, for what it's worth.

Again, MCHC covered this so well, I don't think I really need to go there. Granularity and sensitivity in the HIT systems and EMRs that are out there, that we've encountered so far, cannot mark the data. Extraordinary efforts have been put in place in order to filter it- it's expensive, you know. Most of our initial participants weren't even able to figure out how they would go about only sending medication lists that have behavioral health medications. Or only sending transcribed reports that would have a secondary mention of a behavioral health issue. Consequently, nothing goes. We're just not sharing anything other than demographics, lab results and allergies. Some data is better than no data. At least we've got something, a possibility that a test may not be repeated, or that a physician might look at a previous test result, see that there's been a significant change and we might actually do a patient some good. But without the patient history and everything else that's in there, it's just not as valuable as we'd like it to be.

It was really late at night when I wrote that. Myth of the complete record: In discussing with our initial participants the whole idea about whether or not we could rely on this aggregate record as being the whole health history and the whole record, everybody was very uncomfortable with it. As we really thought about it, it's not really the case now. If you request information, from several providers, there's still a possibility that there's a provider out there who has information on your patient, that your patient has probably forgot about and you don't know about, so you don't have it. As we move forward electronically, we're not going to have 100% participation. There are going to be physicians, and we know of physicians right now, who will not go to an electronic record system and they will retire without an electronic record system. But until that happens, we're not going to have a complete record; So maybe someday down the road when there's some better way of testing and assuring that we've got all the information. We are able to, at least, sequester some of the sensitive labs. Dr. Mark, who is our CMIL, created a list of at least what he knew sensitive labs were at Methodist Medical Center. We shared that with several of the other participants, and they added and subtracted accordingly and they're using that to block according to the lab code description, which results are not being shared that have genetic testing, STDs, etc. And we're not, of course, sharing behavioral health. One thing though that we did think, we do think that if we had an agreement from the IL HIE Authority that it might be possible, we'd have the capability to collect [recording unclear]. If the data is there, why not ask the patient while they're sitting in front of you and obtain a written consent. If that can be managed, and we think it can. In fact, we had the procedures and everything in place to do it, but some of our organizations were just not sure that was good enough, without better direction. So at this particular point, we're not doing that.

[Recording unclear] As far as patient access and error correction are concerned, we still support the idea that the only place you can really correct an error is at the source. So, if we have procedures in place that if there's an error that's detected that the sending organization is advised. They can look at it; they know their data. They can figure out where there really is an error, correct it, and then advise the participants that a correction has been made. Just for your own, an FYI, I did send Marvin, Mary and the team our policies and procedures; our security policies, our privacy policies, and what we call our provider participation kit, which outlines some guidance on how they can operationalize managing consent and how they can describe the security features that they're utilizing, to the patient.

This is the 'Threat Landscape' according to the Office of Civil Right (OCR). This is data that I collected off of the website from their wall of shame, since they began to track this in 2009, after HITECH. What you'll notice is that 59% of the incidents and 68% of the patients are not the result of a hack, data is lost because media was lost. And as we know, with the guidance that came out shortly after HITECH, not encrypted media, because if it's encrypted it's not a disclosure. Credential misuse is the next largest, you know, issue. And that's an issue that I don't think an HIE or even a state party can address. It's an employee management issue. We can help them because in a lot of reports they can validate whether or not a physician's or nurse's use of the data was appropriate. But at this point in time, that's really the best we can do. There is no way for us to be able to automatically determine who an assigned provider is to a particular patient, and have some kind of an automated way of knowing whether someone should or should not be looking at that particular patient. We have to utilize the administrative controls, if you have it in place. And then look at, of course, hacking. 7% of the incidents and only 4% of the patients were actually affected by a hack. So I just think, again, this is not a matter of assuring absolute security for everybody. It never is. All we're doing is managing risk. We need to focus on the areas that are riskiest. And, hacking, we have some fairly sophisticated and fairly well understood methodologies in place to secure the network. Where I think we're really needing to sure things up is with credential misuses and making sure we don't have, you know, the media loss.

That being said, in an effort to produce transparency, we don't want to scare our patient population. We have to be careful about how we present the data. Certainly if there's a breach, but suspected breaches, I don't know where we draw the line. It's just one of those things I would caution you about. So what's the Authority's role? This is just my thought, I wonder if the authority could provide a rick pool, or the liability of breach. That might make it more affordable for all of us in the state. I think that the Authority's role is to validate that we have the appropriate measures in place.

Because of the huge complexity among participants- when you think about participants from a single doc office, all the way up to an IDN- I want to caution the authority on trying to set very, very specific requirements for security. So that it doesn't occur that smaller providers can't be, and yet it's fair and risks are still being addressed. I gave a couple of suggestions there for baselines, my suggestion would be that we follow Nist, because Nist is actually based on the HIPAA and HITECH expectations. We can move towards more sophisticated security standards as things develop, but you know, this is the place to start. So in conclusion, our position on a lot of these issues is, you

know, the Perfect is the enemy of the Good. And Dr. Halamka quotes that quite often. I don't think we're quite ready to engage in some of the activities that we will definitely want to engage in as an HIE. But I hope what we can do, is to clear the path for doing what we can do today and start steering things towards what we want we will be able to do in the future. I'm certainly open for questions- I know that I've overrun the time.

Mark Chudzinski: *Thank you, David. I apologize for cutting into the- sorry deck! Which is distributed to all of the members of the committee and will be posted on the IL HIE website. We are running about half an hour late, but if there are questions right now for Central Illinois HIE…?*

Audience Member #1*: I had a quick question: It was interesting to hear a description of the policies from MetroChicago HIE and then, a contrast description of the policies that are used in the Central one, where the policies are different between the two. And then, when you do the state HIE, the policies may be different again. So for example, your opt out policy was different from the opt out policy of the Chicago area and I assume we'll have an opt out policy if we have opt out, that particular policy variation of this- I guess the question I'm thinking is, how can we learn from the various different choices and how do we keep from confusing patients with a variety of different semantics of opt out, for example. What do you think about the ability to uniformize some of this?*

David Miller: *Well, I think, indeed that's what we're looking for. We want to uniform the standard across the board. I do think that coming up here first, we have really stepped back into the fire, burned ourselves a number of times, it has been very, very difficult. So I would suggest, that especially having this in terms of form of consent, really seems to be working very well and we don't seem to be getting a lot of push back from the patients. One of the things that I shared with Mark, that I'll just briefly mention, on our website CHIE.org or Allchartsnow.com, we have two different sets of patient and stakeholder testimonies. And when you listen to their stories, it's very consistently that they want the data, they want pretty much to freely exchange. So it's a matter of making it easy to share; not making it easy to not share. I know that seems kind of crazy. We don't want to remove choice from people, that's not our intention. But, what we want to favor, what seems to be what most people really, really do want [recording unclear].*

Mark Chudzinski*: Any other questions from the committee members or from the committee members from Springfield or on the web? If not, I'll ask my colleague Mary McGinnis to now do the last Regional HIE and introduce our first panel.*

Mary McGinnis: *Morning, Good morning everybody. I am going to be reading testimony on behalf of Steve Lawrence:*

Good morning I appreciate your willingness to read this testimony into the Committee record.
My name is Steve Lawrence. I am Executive Vice President for the Southern Illinois

Healthcare Foundation, a Federally Qualified Health Center provider that serves eight counties in Southern Illinois. I am presenting testimony in my role as Executive Director for Lincoln Land HIE, which was established as an LLC in 2011 and Illinois Health Exchange Partners, established as an LLC in 2012. The two HIEs have separate governing boards to allow each to respond to unique market requirements in each geography, but share technology, infrastructure, staffing, and administrative services to facilitate a shared sustainability model. Lincoln Land HIE and Illinois Health Exchange Partners have a contract with Medicity to provide the Medicity Novo Grid and iNexx platforms. The two HIEs will cover a large geographic area in central and southern Illinois, and participation in the two HIEs is open any healthcare or community provider in Illinois and the bordering states. Requirements for the products and services offered by the HIEs were identified through extensive field interviews in 70 organizations, hospital departments, and clinics with approximately 200 individuals including physicians, nurse practitioners, lab and radiology techs, nurses, medical records and information technology staff, healthcare executives, hospital department administrators, and community service providers. Through field studies, we identified their clinical workflows, communications, and transitions of care challenges and needs in order to determine the types of technical infrastructure, products, and capabilities required to bring about greater efficiencies, effectiveness, and reliability for clinical information exchange to serve the provider and patient. Because so many physicians practices in our rural communities and in the Metro-East area are largely paper-based, we looked at how we could support them with the HIE network while they transitioned to the electronic exchange environment. We also paid attention to the requirements in environments that already had deployed electronic exchange capacity (largely for the delivery of laboratory results), the scanning volumes in those environments, and the challenges and costs associated with the development and maintenance of point-to-point interfaces.

During our practice-based interviews, physicians repeatedly emphasized that clinical data, including laboratory results, dictated reports, emergency department and inpatient discharge summaries, and other clinical information was needed at the point-of-care delivered directly to the physician's own medical record in order to be the least disruptive to clinician work flow.

Physicians and clinics experienced with e-prescribing also indicated they wanted to be able to generate electronic orders from inside the practice electronic health record system for other types of clinical services, such as mammograms, colonoscopies, laboratory tests, and procedures. Hospitals were interested in this capability as well in order to ensure accurate and complete information about the patient presenting for services and the type of test needed, and to reduce the number of calls backs to the clinics to clarify orders and instructions, all of which contribute to the inefficiencies we are working hard to eliminate in healthcare delivery today. Electronic orders and results provide greater efficiencies, effectiveness, and reliability over the manual environment today. The HIEs can also audit records and tell a hospital or physician exactly when a transaction for a clinical communication was delivered to its intended recipient.

Physicians and clinic referrals staff will also be able to electronically submit and manage referrals through the HIE network, thereby addressing one of the key issues that

creates significant call back activity and delays in care due to both missing information from the referring physician and not knowing the actions were taken by the consulting physician. We will provide an electronic infrastructure to set up unique "virtual" patient care teams allowing medical homes, hospital discharge planners, and other healthcare providers to efficiently coordinate and transition care between and among all members of the medical team for patients with chronic conditions or who are at high-risk for an avoidable readmission.

Our founders and stakeholders determined that electronic orders, results, and referrals were the highest priority for implementation. Health system and hospital CEOs that participated in the building of the necessary social capital to establish and financially sustain these use cases met critical business requirements and clinical needs. We do not have plans to implement a centralized community database with an Master Patient Index or Record Locator Service as this was not a priority for our founders at this time because their physicians did not want to have to seek patient information from another portal outside of the practice electronic health record system. Lincoln Land HIE will be in production later this summer, and ILHEP will be in production sometime late fall.

Lincoln Land HIE and ILHEP each engaged with Steve Gravely and Erin Whaley of Troutman Sanders as our legal counsel because of their expertise in health information exchange and their experience working MedVirginia and other HIEs around the country. Steve Gravely was the chief architect of the Data Use and Reciprocal Support Agreement also known as the DURSA which is the comprehensive, multi-party trust agreement signed by those participating in the Nationwide Health Information Network. Together they led Lincoln Land HIE and ILHEP through a similar trust framework process. Mr. Gravely and Ms. Whaley developed our agreements, policies, and procedures including those pertaining to privacy and security. The policies and procedures are compliant with state and federal laws and are comprehensive in addressing legal, operational, privacy, and security matters. The policies and procedures cover workforce member confidentiality and compliance, discipline, breach notification, business associate agreements, uses and disclosures of PHI, the minimum necessary standard, accounting disclosures, security risk management, suspension and termination procedures, security awareness and training, malicious software, log-in monitoring, password management, contingency plan, data backup and disaster recovery plans, emergency mode operation plan, evaluation of security policies and procedures, facility access and security, person or entity authentication, transmission security, data integrity, and others in the comprehensive manual. In addition, each participant in the HIE Network is required to sign a comprehensive participation agreement that outlines privacy and security obligations and responsibilities and acknowledges that they will abide by the policies and procedures of the HIEs.

I appreciate the opportunity to provide this testimony. You will be hearing from Dr. David Graham, chair of the Lincoln Land HIE and Dr. Tom Mikkelson, chair of ILHEP. They will covering specific questions pertaining to the panels and will be able to answer your questions at that time.

V. Testimonies – (11:00am-12:00pm)

Patient Choice: Options and Permitted Uses for Patient Data

Granularity of Patient Data

***Mary McGinnis**: At this time I'd like to welcome Sonia Desai to the podium, and she is going to present a paper about Patient Choice: Options and Permitted Uses for Patient Data. This will be the opening session of our testimony, so Sonia, please.*

***Sonia Desai**: Thank you, Mary. You've all already heard, you know, delved in to these issues already, so I'll be very brief and quick. You know, we just wanted to take a step back before we started the actual Panel One testimonies to very briefly look more broadly at some of the, you know, major policy issues that this group will be tackling and give some basic overview. So going to the next slide..*

The issue of how much patient control there should be over health data exchange in an HIE is at the forefront of policy challenges for HIEs, as we've already heard. There are a number of factors to look at and the people from the Regional HIEs have touched on number of them. But, you know, the first issue is should patients be given a choice at all whether their health data can be part of an HIE? Or should we just go with what HIPAA does? Is HIPAA enough? Number two, if the patients are given a choice beyond HIPAA, should all patients be provided the option affirmatively consent to HIE inclusion ("opt-in") or should their health data be included automatically unless they affirmatively decline inclusion ("opt-out")? And of course there are variations of them.

The third major issue is granularity. We've heard about that already. Should patients have the ability to sequester specific elements of their patient record from specific providers ("granularity") or should the entire patient record be excluded from the HIE if a patient desires some data be sequestered ("all in or all out")? And the fourth major issue is if someone chooses not to participate in HIE. You know, whether data should be entirely excluded from the HIE or should it just not be visible. If a patient chooses against use of the HIE, may the data still be collected by/made accessible to the HIE for mandatory public health reporting or for emergency medical treatment? What's been talked about is the 'break the glass' exception. So those are the major issues that you'll be tackling. And then there are plenty of sub-issues that fall under those.

As you know, current federal law's HIPAA, Federal HIPAA Privacy Rule requires that patient consent is given for all PHI disclosures unless it is otherwise expressly permitted. However, there is an exception. An exception exists for certain disclosures for purposes of "Treatment, Payment and Healthcare Operations", what we call the T-P-O exception. There's also exceptions for public health activities, for research purposes and for other legally required disclosures such as public health reporting of certain diagnosis. So that's what's already in place. And as you've heard plenty about and you will after this, especially protected health information, you know, is different. Illinois, like many other states, have inactive laws that provide heightened privacy protection for certain data: mental health data, substance abuse data, HIV/AIDS data, genetic testing and other data. And these statutes impose more stringent patient consent requirements. So, that's another level of challenge we have.

Some of our federal agencies have spoken on the issue. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has been of the view that patient data can be transmitted through an HIE for treatment purposes without the need of a prior

patient consent. You know, so not even requiring "opt in" or "opt out", that would optional under their view. HHS Centers for Medicare & Medicaid Services (CMS) in 2011 issued rules regarding Accountable Care Organizations (ACO) which encourage the sharing of patient data among participants using a patient "opt-out" system, and that would be the case even for T-P-O purposes. Most recently, HHS Office of National Coordinator for Health Information Technology (ONC) recently issued guidance that patients should be provided a "meaningful choice", either on an "opt-in" or "opt-out" basis, this would be the case even for T-P-O purposes- even if it is for treatment purposes. Meaningful choice, of course refers to a patient making a choice based on some meaningful exchange of information they receive about the HIE.

A number of people this morning have already touched on the various consent models. But to take a step back and get some basic overview, there are five core consent models for health data that have been identified and the models fall in to three broad categories that have been discussed, which are "opt-in", "opt-out" or "no consent. (1) No-consent: Health data is automatically eligible for exchange by the HIE without requiring patient consent. However, you'd still have to adhere to HIPAA regulations. (2) Opt-out: Health data is automatically eligible for inclusion in the HIE, but each patient must be given the opportunity to opt-out in full. (3) There's also opt-out with exceptions: Health data is automatically included in the HIE unless patients opt out. Patients can choose to opt out in full, or under this model you're given the choice to limit the extent of inclusion. They can exclude specific data, limit the flow of data to specific providers or organizations, or allow the exchange only for specific purposes. (4) Opt-in: Patient consent is required to have health data included in/transmitted through the HIE. (5) Opt-in with restrictions: Patient consent is required to have health data included in the HIE. Patients may also choose which data is included, which providers or organization can receive the data and the specific purposes for the exchange. There are a number of pros and cons of each model that I was going to go through, but in the interest of time we'll move on, because we'll hear about them from our panelists.

So looking nationally at what the current landscape is: 27 states currently have adopted an opt-out type of model; 12 states have adopted an opt-in model; No consent is required in 3 states and 8 states are still determining the issue. Okay, I'll turn it over to the panelists to expand further. Thank you.

***Mary McGinnis**: Good morning- it's still morning. We appreciate everybody's time and patience. The good news is we have a lot of testimony and a lot of input. We're going to switch up the order because we've got some folks with some time constraints. So I'd like to welcome Mr. Ira Thompson from Intersystems Services for his testimony please.*

***Ira Thompson:** Thank you very much. In the interest of time, I'm going to give you the highlights. I have the pleasure to think about this committee. And I'm actually going to do a quick tag-team. I'm going to have a few quick remarks and then I'm going toturn it over to my business partner, Mr. Ronald Warren, who's the CIO of Loretto Hospital as well.*

We've talked a lot about HIPAA, the HIPAA standards and requirements. One of the basic ones is HIPAA Security Standard 164312: the Order and Control Standard requires the

covered entity to implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. That standard also states that the health insurance protocol is- The HIPAA standard also requires the covered entity have a mechanism for notifying, having detecting control in place that record and examine activity

left off at 1:49:47
Ira speaks until 1:51

Ronald Warren:

Hi, thank you for this opportunity. I'm just going to be very brief. We do have some position papers as they relate to governance. It's our perspective that all the framework should be standards based and compliance governed. It's one thing to have a standard that says 'this is what we should do' , but without some type of governance to ensure there's compliance, there's no real reliability or credibility to that assessment, if there's no real assessment done. We find that misuse of gatekeeper laws are generally more detected after the fact, than preventative. And the control framework must consist of both. You must have the preventative controls which are looking at the design of what you're doing. And then the operational controls that detect whether or not it's working as designed.

Our research also indicates that there are approaches to mental health data that put the patient's health first. And that's one of the concerns that we've seen in this area. We say our number one objective is the patient, but I propose that it goes deeper than that. I think it warrants the question, what's more important- the patient itself or the patient's security of their information. So you've got to take it down to another level and look at, yeah the patient is the objective but is it more important that we make sure they're healthy by knowing all the components of their condition. Or is it more important that we protect their information so that the people who could use it to help them don't even have access to it? And I think that's a challenge that everyone is facing.

Our perspective is that there's a lot of concern around the sensitivity of data sharing, and that's due to the lack of structure. You're not comfortable that who you give your data to they're going to be responsible, and they're going to be monitored and they're going to be held to a standard of compliance. Without that it's like giving someone your check book and saying 'I trust that you won't write any checks, even though I don't have a signature identified'. So you're kind of leaving yourself open, no patient is going to do that without some assurance. And it's the responsibility of the providers and of the state to ensure that that's in place.

So there are a couple of objectives, a couple of options that you can do to ensure or to better control that. But we believe that a monitoring and compliance program is essential to ensuring the protection of patient information. And the state has a responsibility to make sure that happens for anyone that opts in to the state HIE.

Finally, we talk a lot about the patients and their access to data and whether they give consent. I haven't heard any real methodologies about how about giving the patient their data, how about giving them a chip or giving them a card- a smart card with their information. They can opt to give it to the vendor if they want the vendor to see it. You could do automatic downloads or uploads on a multi-bases and you provide that information so

they're in control of their potentially sensitive information; particularly as it relates to behavioral health. Those are just a few of the perspectives. We understand time is short and appreciate the opportunity to present to the group. If there are any questions, Ira will take them.

***Mary McGinnis**: Thank you, Ron and Ira. Again, we thank you for staying, hanging in there with us so that you could present. We appreciate that. Now I'd like to invite Mr. Marvin Lindsey to the podium. Marvin is from the Community Behavioral Health Association and he will be providing some insight from his organization.*

***Marvin Lindsey**: Thanks Mary. I'm going to be quick; my stomach is talking to me. So, I'm also the Co-Chair of the ILHIE Advisory Committee's Behavioral Health Workgroup, but I'll be speaking mainly as a staff member of CBHA. CBHA is a trade association of about seventy behavioral health care providers around the state. They provide prevention, recovery and treatment services. So I thank you for this opportunity.*

CBHA endorses a broad statewide health integration agenda to provoke better coordinated, less fragmented care. We support a coordinated system of care that can lead to improvements of patient health outcome, accountability, make access for patients more efficient and effective, promote cost savings for local and state taxpayers, consumers, and providers. Individuals requiring behavioral health services have a unique need for integrated care due to frequent use of the health care system. And a greater need to coordinate care among diverse providers. Many CBHA members have developed proven effective models that integrate care to treat individuals with behavioral health and medical [recording unclear]. CBHA believes that the CHIE can assist these through sharing critical patient information such a medical history, medication list, to better coordinate patient care. CBHA recognizes that access to comprehensive patient health record, which include behavioral health information is important to in providing quality care and achieving desirable outcomes. We view the electronic exchange of patient data and the HIE as one of the means to accomplish the desired health outcomes; but should not outweigh the potential privacy and confidentiality concerns.

In light of that, CBHA would like to just briefly focus a little bit of our testimony on informed consent policies and sharing behavioral health data. CBHA recommends informed consent policy that allows patient choice and clearly informs the patient- or someone authorized to act on the behalf of the patient- the exact purpose of the use of their patient information. Due to the complexities of issues involved in selecting and applying a particular consent model, appropriate guidance in the form of high level principles is critical to moving forward. We also urge the development of consent management function within the HIE that can accommodate variant consent directives. In order for the behavioral health community to fully participate in the HIE, either using an opt in or an opt out model, CBHA understands that certain state and federal laws will need to be amended. It is our position that the HIE patient consent policies should not be a barrier to information sharing or to the inclusion of the behavioral health community in the HIE. But the choice of participation should be in the hands of an informed patient or their representative. Patients must be assured that appropriate technology solutions, business practices, and policy protections will be employed to prevent their information from being used in undesirable ways or to infringe upon their

rights and civil liberties. And that it will be used exactly in the ways agreed upon.

And lastly, CBHA views the electronic sharing of behavioral health patient information within a coordinated network of providers as essential to optimal health and care. We recommend the sharing of behavioral health history, medications and treatment within the HIE. And the development of policies that allow patients the ability to sequester their behavioral health records from specific providers that are not involved in their immediate care. Any health care providers providing emergency treatment services should be allowed access to patients' entire medical record in order to best serve that patient. Public health officials should also be granted access, strictly for the purpose of population health planning and evaluations.

That's it for our testimony. I also have, I don't know if you have it, but I can make sure you get it, it's an executive summary from a March 2011 survey on HI consent or behavioral health care providers that was conducted by the behavioral health work group. And I thank you for this opportunity.

***Mark Chudzinski**: Thank you.*

***Mary McGinnis**: Are there any questions for Marvin, Mr. Lindsey? Yes, Dr. Gunter…*

***Carl Gunter**: I had a question for you. So, as I heard you speaking there, it seemed CBHA is advocating that the health exchange support is sharing not only of the records- people who have mental health records but, the mental health records themselves. Which is more than has been achieved by regional exchanges and so there's some technical challenges with that. And am I understanding you correctly that what you want is for those technical challenges to be overcome so that those records can be shared?*

***Marvin Lindsey**: Exactly.*

***Audience Member**: And legal challenges, right?*

***Marvin Lindsey:** The legal and the technical. Mostly legal at this point, that, you know, has to be worked out. But our organization understands that certain changes need to be made and will probably advocate for those changes.*

***Audience Member**: And I just want to understand who your organization is. It's an association of all the community behavioral health providers, or most of the community behavioral health providers?*

***Marvin Lindsey**: We are the largest behavioral health care trade association. So we have seventy members statewide, all the way from Cairo, Illinois to Lake County.*

***Audience Member**: Yeah, I wanted to clarify on the technical and legal issue. The legal issue here is there's a very restrictive state law that's making an impediment to using exchange. The technical impediment is that it's hard to figure out which part of the record is the mental health record. So if you want to have some sort of special treatment of that data, it's*

technically difficult to do that.

Mary McGinnis: *Any other questions for Mr. Lindsey? Again Marvin, thank you very much for your testimony. I'd like to next welcome Ann Hilton Fisher to the podium. Ann is with the AIDS Legal Council of Chicago.*

Ann Hilton Fisher*: Thank you. I'm here on behalf of the AIDS Legal Council which is the largest provider of direct legal services to people with HIV and AIDS. And I have also here with me Ramon Gardenheir, who is with the AIDS Foundation of Chicago, which is really the statewide leader generally in providing services to people with HIV/AIDS. I'm not going to do a lot of introductory stuff. You've all worked very hard on these issues.*

I want to say, Illinois has the nation's best HIV confidentiality laws. And we have them for a reason. We have them for a public health reason, because as the law itself says, as everywhere- whether you're talking about somebody providing HIV services in Malawai or on the West Side of Chicago, we know that people will not come in to get tested and will not come in and get care if they fear that information will be disclosed without their consent. People are not burning down the houses of people with HIV anymore, but there is still enormous stigma and discrimination. As the AIDS Legal Council, we see it at work every day, every week. I wish I could say it never came from health care providers, I cannot say that. Health care providers read the same things everybody else reads and have some of the same fears. We also know that a lot of the stigma gets internalized. So that if you're telling a group of people that they're worthless and they have, you know, they're promiscuous and drug addicts, they too will begin to feel worthless and become reluctant to seek out medical care.

So we have this public health purpose. Our public health purpose is you've got to protect confidentiality to encourage people to come in and to get tested and treated. We had that rule before we even had any treatment. When we first had a test for HIV, we said 'Okay, we're going to put very strict confidentiality on this'. We now have good treatment for HIV, very valuable treatment for HIV. We're in an era now where we discovered if in fact we could find the people with HIV, identify them and bring them in to treatment, then we can stop the spread of HIV. We can drive down a community viral load and reduce generally the incidents of HIV within a community if we can just identify the people who have it.

So there's a lot of emphasis going on everywhere in the country on finding people and bringing them in to treatment. The catch is this is not treatment for Syphilis, with one shot and you're better. This is not even treatment for tuberculosis where for six months a public health nurse comes to your house and makes sure you take your medication and then you're no longer going to spread that tuberculosis. HIV treatment today requires absolute, 95%, plus adherence to medications, regular lab work, there's a lot of drug resistance. It requires a lifelong, very strict commitment to a treatment with a lot of bad side effects. What we know- and there are some phenomenal HIV treatment providers in this state- is that it requires a very close trusting relationship between the person with HIV and the provider. And so that's where we're starting from, that's what we need to make sure happens. We know a lot of people get tested and never show up in care, or people start treatment and drop out. We want to bring those people back, we want to make it safe for those people to come back.

So the key to our HIV confidentiality law is that an individual has control of their

medical data. And of course, this comes as no surprise, it's a pretty fundamental principle. And I will tell you that we work pretty close with the ACLU on a lot of these issues. I know you're going to hear from Colleen Connell, who will give you a lot more detail on some of these topics. But basically, our law says that a person's HIV information is theirs to share, with some very limited restrictions. And if we're going to keep that in an era of- in the Illinois health exchange, we have to pay very close attention to the same topics you've been hearing about all morning, and you'll hear about all afternoon: Informed consent patient choice. I think that that's really going to require, and this is the position of the AIDS Legal Council and AIDS Foundation of Chicago, that it's got to be an opt in process, it's affirmatively- I mean all of us have had a million sort of statements of privacy practices shoved across our desks and that's not giving us any meaningful information. Even an opt out, depending on how it's done can be pretty sloppy. Opt in requires a conversation, requires some affirmative 'Yes I know this is happening, yes this is okay with me'. We know from the world of HIV testing that opt in may not be a barrier and in fact, if you've got a trusting relationship, you can get opt in consent.

We do agree that there ought to be a way to sequester sensitive information, including HIV information. I absolutely understand that there's some incredible technical challenges to doing that. But it sounds like people are working on leading those challenges. I would encourage that work to go on.

Something that I've not heard talked about, I heard a little bit in one of the presentations this morning and I apologize for not being here for all of it. I think a real key piece is the consent at the other end. That that's really the point at which you're giving the person the ability to say 'You're in an emergency room, you've got something, is it okay if I go see what records we can find for you on the information exchange?'. That's the point in which the person can say 'Oh my god, yes, I can now remember my medications. I know I had a viral load test, I can't tell you what it was, please go get that information.'. Or ' No, I'm here for a broken arm. I don't particularly want all of my family health history all of it out here at this particular presentation'. So another opportunity to consent and perhaps the most important opportunity to consent is coming at that point when that information is going to be used.

So that's a lot of the basics. I do want to stress again- and I do stress this in my materials which I hope you've gotten or if not will get- that there has to be the ability to correct information, and I hear people have been addressing that. We do get some regularity, people whose medical record show they're HIV positive, when they in fact are not. Because we have screening tests, like a lot of screening tests, that sometimes produce false positives. We obviously need to be able to get in to those records and correct that.

So I think we've got some work to do. I think the panel has been on the right track, in terms of working on this. But I really encourage you to listen to the presentation from the ACLU and really think about how we can really preserve patient choice, patient autonomy, in this era that can be very, very important of access to information. Thank you.

***Mary McGinnis**: Are there any questions for Ms. Fisher?*

***Audience Member**: Thank you for your testimony. I'm just looking at your written materials and I noticed the quote on stigma and you mentioned stigma being the biggest barrier in*

treatment for HIV/AIDS. From a policy perspective, is it more valuable to continue to maintain HIV/AIDS information as separate to segregate it from other information, to keep it more protected and more secret than other health information? Would that in your opinion, or in your organization's opinion, limit or desensitize people to this stigma or would it be better to actually treat it as the medical condition that it is?

***Ann Hilton Fisher**: Thank you. I've heard that argument a lot, that somehow the fact that we have these laws are what's creating the stigma. I can assure you that I don't think a single case of discrimination, that I've seen in my office, has been caused by somebody saying 'Oh, there's a special law about HIV therefore it must be a terrible disease'. There's stigma associated with this disease because it's associated with homosexuality, with drug use, with sex workers, with a very marginalized community. The stigma absolutely exists, prevails, the law is the result of the stigma, the stigma is not the result of the law. The stigma continues the protection must continue.*

***Mary McGinnis:** Are there questions for Ms. Fisher? Thank you very much for your testimony. I'd like to welcome Mr. Peter Eckart to the podium. Peter is with the Illinois Public Health Institute.*

***Peter Eckart**: Good afternoon. I'm Peter Eckart, I'm the director of health information technology at the Illinois Public Health Institute and if that sounds familiar to you, it's because the CEO of that organization is sitting at your table, Elissa Bassler. But on behalf of Elissa and the board, we're happy to provide testimony this morning.*

From 2007-2009, IPHI staffed Illinois' participation in the national Health Information Security and Privacy Collaborative (IL-HISPC), an early federal initiative to address privacy and security in the (then) upcoming world of inter-connected electronic medical records. In 2009, IPHI started working with Illinois' Office of Health Information Technology, when it was still with IDHFS. We monitored and supported the regional planning processes for the sixteen medical trading areas that eventually led to the creation of Illinois' regional HIEs. In 2010, IPHI helped to form the statewide Illinois Health Information Technology Regional Extension Center (IL-HITREC) that provides services and support to healthcare providers installing or upgrading medical record systems. IPHI created and staffed the online training platform to support that initiative.

Finally, for the last fifteen months, IPHI has worked with the Illinois Department of Human Services on the Illinois Health and Human Services Framework, an initiative that seeks to integrate the client and provider information systems of seven state agencies, including DHS, HFS, DCFS, IDES, DCEO, IDPH, and Aging. On behalf of the Framework, IPHI hosted 25 Listening Tour conversations with service recipients and community providers, in order to introduce the idea of the Framework to these important stakeholders and to gather their feedback about the impact of state agency systems in their lives.

IPHI CEO Elissa Bassler serves on the HIE Authority Advisory Committee and this Privacy and Security Sub-committee. I serve on two OHIT working groups – on public health and consumer education – and formerly served on the OHIT Privacy and Security Working Group that preceded this committee's work.

Over the course of our involvement in public efforts leading to the development of the

ILHIE, IPHI has developed expertise and opinions on many of the questions before these panels. Today, we're focusing our remarks on the topic of options and permitted uses for patient data.

IPHI strongly favors the opt-out model of patient consent: all patients should be given the option to opt out of electronic medical record and health information exchange systems. To be clear, we are saying that the Illinois HIE and its affiliated regional exchanges should make patient data available through the ILHIE and among the regional exchanges as its default policy. We believe that this creates concomitant obligations on the part of the state/exchange operators to secure patient data as strongly as possible, and to restrict access to this data to only those who need it for valid medical or operational reasons.

The Opt-Out approach is important to the efficient and effective operation of the HIE. It is also critical to ensuring the highest quality of patient care; without access to medical records, physicians and other health professionals are less able to make appropriate diagnoses and treatment decisions.

However, IPHI believes there is another critical public good that is at stake in this decision. Improving health at the population level – across groups of people rather than the individual level – is the mission of public health. Examples include: clean, potable water reduces disease among everyone who drinks it; improving the nutritional quality of school lunches helps all students be healthier. Public health is reliant on aggregated, not individual, data for understanding what health problems are affecting which groups of people and where. Data helps public health plan population-level interventions, evaluate the efficacy of public health programs, and advocate for policies that improve the public's health.

The success of health care reform is dependent on people being healthier/less sick overall. On the clinical side, that is why there is such focus on primary care and preventive services. It is also why there is a significant focus in the ACA in strengthening population health outcomes. IPHI sees the Illinois HIE as a new and powerful mechanism that will improve our understanding of the health of Illinois residents and sub-groups within the population. Simply put, more and better data can lead to better outcomes, and comprehensive data leads to the best outcomes. Opt-out consent is likely to lead to the highest percentage of residents participating in the Exchange, which will give us the most detailed descriptions of the health of our communities. That is why we support it.

Let me make clear that for the purposes I describe, we do not need access to individual patient data. Public health works with population level data, which means that we count up the occurrences of a particular health indicator across a group or the whole population, and then analyze the data to understand trends, emerging health issues, and disparately affected groups, whether defined as a geographic community, a racial or ethnic group, or age group. Then we plan and implement interventions that can reduce the burden of disease in the group or population. Comprehensive aggregated data is the key to better policies and healthier people.

Obesity as an example: The current public attention to obesity gives us a good way to understand how comprehensive data supports good policy making and program design. In the last few years, we have come to understand obesity as an epidemic that is sweeping the country. Perhaps you are familiar with the famous set of slides from the CDC that show a map of the percentage of obese Americans state by state over the last 25 years. In 1985, eight states reported the highest level of obesity, with 10-14% of residents significantly

overweight. Over time, the maps add colors to represent 15%, then 20%, then 25%. By 2010, 13 states have an obese population equal to or greater than 30%, and no state is below 20%. As percentages of overweight and obesity increase each year, the map gets darker and darker, showing simply and clearly how pervasive a problem this has become for the entire country. That's the power of comprehensive health data.

Now, imagine that we have that same kind of data in Illinois, but available at a much finer level of detail. Most EMRs will contain height and weight measurements (along with age and gender), which gives us an indicator of being overweight or obese: body mass index (BMI). When that BMI data is available in an individual's medical record, that provider can quickly evaluate that individual patients' danger for overweight and obesity.

When that BMI data is available within the HIE, it can be added to BMI data for patients across the community and across the state, and reported back by community, age, race, ethnicity, health status, and a host of other factors. When combined with other analyses – such as available parks and recreation, crime statistics, access to health foods, educational attainment, employment data, and other community characteristics– we can pinpoint the places and populations where obesity is most prevalent, and also start to understand the reasons why it is better in one place or worse in another. With comprehensive aggregated data, we can design programs that target the highest risk communities, and also have the means to evaluate the effectiveness of those interventions.

In conclusion, public health has long been a leader in generating, collecting and disseminating information about the health of communities. Public health deals in whole populations, and this population-level data is hard to come by. The opt-out policy of consent health information exchange will result in as comprehensive a set of data as possible. We have the opportunity to aggregate the data about the residents of Illinois, and help them to be healthier overall – a public goal that will help save lives and conserve resources. Thank you.

Audience Member: *Thank you for the testimony. You were very clear on the opt-in, opt-out area. But listening to some of the other discussions of health information exchanges, not just in our state but in other states, sometimes the providers are not very keen on research done- that is data being extracted from the health information exchange. There might be a risk that if the health information exchange did much of that, the providers might be willing to participate. I wonder what you thought of that or is that going to be an issue? And how are we going to overcome that if it is an issue?*

Peter Eckart*: I appreciate that as an issue, both kind of short term and long term. My initial reaction is probably that providers have traditionally been first about securing their own systems and working to greater quality and greater efficiency. And sort of, the secondary use of their data has not been a concern for them. I think that Dr. Shen's comment earlier and the statement that some Regional HIE people made earlier about being interested and committed in public use of the data. In the long term, I think it's something that sort of everybody agrees to. But I think it's sort of the short term place that where we are now which is (A) How would we pay for the necessary expenses and then how do we handle some of these growing question about privacy and then of course the technical issues. So, I would say that reticence that you're describing on the part of providers, it may be about their*

concerns about some of the things we just talked about. But it may also be relatively early in the process of interconnecting theses systems and working towards secondary use of this data.

Mary McGinnis: *Any other question for Mr. Eckart?*

Audience Member*: I'll just follow up. I don't want to put word in your mouth, but maybe one thing that you're saying here is that at a very minimum when we do the Illinois health information exchange, it would be good if there was some sort of governance system that would show a pathway to public health uses of the data. Even if, maybe, that can't just be made available immediately.*

Peter Eckart*: Well, I think that that's exactly right. I'll say that IPHI Health Information Technology does have a public health working group. And I'm on it and some of my colleagues who have spoken or will speak are on it. The public health community broadly gathered has been struggling with this issue. In a very specific way we refer to it as Public Health Data Node. And so, this is something that in a non specific way has already been considered. I think one of the reasons for our testimony today is to represent the fact that we kind of recognize, in a realistic way, that the secondary use of this data- whether for research purposes or public health population assessment and advocacy and assurance, may not be part of the infrastructure building today, or even next year. But we want to continue to raise it because the potential use of this comprehensive data is so powerful.*

Audience Member*: Not to get too bugged down on the details. But could you speak a little bit to how the actual technical aspect of this public health concentration or review would work with the structure, or the proposed structure, of ILHIE being kind of a federated mount rather than a central bucket of information that you could apply theses searches to.*

Peter Eckart: *No. You know, one of the things that I was struck by is I heard the three presentations from the Regional Exchanges is that, you know, they are still so early in their definition. In fact, they're not doing a lot of what they want to do just for their own governance and purposes. Not to kick the ball too far down the field, but I think one of the things that has to happen is that if we're not raising the use of these systems- if we're not raising the access to aggregated public health data right now, while we're still getting started we're not going to be able to sort of understand what the technical exclusions will eventually be. People have talked about a public health data warehouse, where you would pull out aggregated data and it sit there [recording unclear]. We've talked about sort of being able to give public health its ability to pop in to the federated model and do queries that result in aggregated de-identified data. There are technical people who are asking these questions. And I think that one of the things that we say is if we are articulating communally and corporately a priority for eventual use of this data, as a source for population health analysis that we'll figure that question out. The same way that we'll eventually figure out all of these sort of questions.*

Mary McGinnis*: Any other questions for Peter? Thank you so much Peter. I'd like to welcome*

Mr. Gregory Ignatius to the podium. Mr. Ignatius is a Patient Advocate.

***Gregory Ignatius**:*

Hello and thank you for the opportunity to discuss some of my concerns about health information exchange. To briefly introduce myself, for most of my professional years I worked as a systems and software engineer for fortune 100 companies mostly in telecommunications. I am here today to describe what I believe is important related to electronic health information exchange and privacy. My extensive technology background leads me to a very different opinion about this topic than you may hear from others. Privacy and HIPAA are cited as reasons why electronic exchange of health information should not be done or limited. This is a red herring. As a patient the first thing I am always required to do is to sign a form giving the health care provider the ability to send my health information to an insurance company so the provider can get paid. If they aren't paid, that form lets them send the information to a collection agency.

Here's reality. I was evaluated by a Neuro psychologist on multiple occasions, and he would only give his reports to my primary care doctor. He would not give them to me. These reports contain lots of very detailed private information about me, sexual behavior, my emotions, and my concerns. They also included information about finger tapping and the grooved pegboard test for fine motor control, and later those would be crucial. Multiple times I was referred to specialists for different reasons. Each time I asked the Neuro psychologist to fax the reports to the physician I was going to see. I knew these were faxed over unsecured, ordinary fax lines. Most in health care don't even know what a secure fax line is. I would get to an appointment, after waiting 3 months or more, and the doctor did not have the reports. I finally started insisting that I be given copies of the reports that I could carry with me. There were at least four different occasions when I showed up for an appointment, the neuro psych report was supposed to have been faxed, and the doctor said they did not receive anything.

These neuro psych reports held extensive, subjective information about me including the evaluator's critical perceptions of my psychosocial mal-adjustments and his notions about my inadequacies as a human being. I do believe that the psychologist did fax the reports, yet repeatedly, they were never received. I have no idea what actually happened to the faxes. I suspect that because the doctor I was to see did not have me as an existing patient, the reports ended up in a pile next to the fax machine. For all I know those reports could have been sold to Julian Assange to be posted on Wiki-leaks. Repeatedly they were sent, and did not reach the intended destination. What is done now largely uses unsecured fax lines, and unexpected, unrecognized transmissions probably are not even shredded. I'm willing to bet that most offices toss them in a recycle bin.

I have had similar experiences with test results for blood work, reports from neurologists, and medical record notes. Sometimes the neurologist's report would be saying that I was neurotic or otherwise of doubtful sanity, and I probably still am, but the reality was these reports would be faxed, and when I would show up for an appointment, they didn't have it. The only reason the appointment could continue, was that I learned to always make sure that I had copies of test results, reports, and doctor's notes in my hand which I could give to the doctor I was seeing.

Those test results disclosed all kinds sensitive intimate information, frequently with

my name and social security number on them, and no one could tell me what happened to the fax. Everyone shrugged it off as if it was nothing. At the same time, detailed personal information about me was routinely sent to the insurance company so they could determine whether or not to pay for something.

Along the way, twice I had falls with a broken arm and a broken leg, each required an emergency room visit. I remember being in the middle of a very public ER area, where the intake person loudly demanded to know what medications I was on. Suddenly I was a spectacle with prying eyes all around morbidly curious to hear my answer.

I need to fast forward here. A couple years ago I was diagnosed with Parkinson's. Even in the early stages of Parkinson's the disorder changes your personality and negatively impacts your cognitive function. It is very stressful to repeatedly go to doctor's appointments and be told that you have deep seated psychological problems, and I knew in my core that's not why my hand was shaking. Parkinson's, not insanity also explained why I had difficulty walking, and would fall ending up with broken bones. Stress makes my cognitive issues worse, my hands shake more, and sometimes I completely freeze up, I don't know where I am, how I got there, or what I'm supposed to be doing. That's in part what my service dog helps me with.

Because of my complex medical situation, I have ended up seeing many doctors. Recently I was seen by several specialists who I then asked to send reports to my primary care doctor. He was not getting those reports. When I asked if this could be done electronically, I heard things like, "Oh we don't do that." Mostly I just wanted them sent, but electronic exchanges can be encrypted and secure.

At a conference for Parkinson's patients I asked a question, "What is the best way to get coordinated care when you have to deal with multiple physicians?" The doctor who responded, said that it was up to me as the patient to make sure that all the treating specialists had the information about me that they needed to treat me. I'm not a doctor, I don't have medical training. How am I supposed to make sure that they have what they need? I deal with medication induced hallucinations of bunny rabbits, blackbirds and bugs, (Sinemet is known to trigger hallucinations) but I'm supposed to make sure the doctor has the right information. Electronic exchange gives the option of sending complete records, and it can be done with encryption so it is genuinely secure.

I worked with my primary care doctor to make sure that a complete list of all my medications was on his electronic health record system. I went for a colonoscopy which requires general anaesthesia. On the hospital's paper form, I wrote that all the medication and drug allergy information was on the doctor's system that they had access to. The intake nurse asked me if I could verbally give her the list of medications because the little room we were in did not have a terminal. She seemed genuinely put out when I insisted that she had to go look them up. Later after they gave me twilight drugs, as I was being wheeled into the procedure room, another nurse asks for my drug allergies. I have been clinically diagnosed with cognitive impairment. I am not a reliable repository for this information, nor am I a reliable transmission means. Yet clearly the expectation was that I the patient should be able to recite this information on queue.

I take so many different prescriptions that no pharmacy system automatically keeps a complete list of all of them. Yet I'm expected to be a walking repository for this information. About a month ago I was prescribed a drug and had a negative reaction to it. My primary

care doctor did not know what to tell me because he didn't have notes from the prescribing specialist, who was out of the office at a conference. I was in distress and not sure what to do. I was asking questions like, "When is it bad enough that I should go to the emergency room?" "If I go to the ER, how will they be able to get enough information about me, to treat me effectively?" The reality was, if I went to the ER, they would just be shooting in the dark trying to figure out what might be going on.

Not having a way to exchange health care information electronically makes it almost certain that I will get wrong care if I ever do need to go to an emergency room. Too many fear mongers dance with the fig leaf of privacy protection required by HIPAA to justify withholding information, while the same data are being faxed over unsecured lines to places where for all I know recipients could be posting it on the web.

I may still be a grumpy old man lacking in social skills, but this situation is nuts. We need robust electronic health information exchange. What happens now makes privacy a joke. What is being done now, does nothing to protect my privacy, really, and it does create a situation where health care professionals must just shoot in the dark. Electronic health information exchange offers that, because we are approaching privacy issues with eyes wide open, we can only make the situation better.

Colleen K. Connell, the Executive Director of the American Civil Liberties Union (ACLU), provided the group with recommendations for the privacy, security, and consent management policies that may well govern the Illinois Health Information Exchange (ILHIE):

Good afternoon, thank you very much. My name is Colleen Connell, as Mary indicated. I am the Executive Director of the ACLU of Illinois, which has 20,000 supporters and members here in Illinois and 500,000 nationwide. Much of the ACLU's work over the past 40 years, actually much of my work over the past 30 years, has been on the issue of privacy protection and privacy concern of patients in some of the more sensitive areas of healthcare: reproductive rights, specifically abortion and contraception, HIV and the transmission of AIDS, and issues involving the medical care of survivor of sexual assault. So I have submitted, and I can see from Mr. notebook that you have my testimony circulated. So what I would like to do is go over my hot points in the interest of time and how long the committee has been here.

The first thing I want to say, like every other speaker up here, is that the key to IL HIE is making certain that each patient has the meaningful opportunity to give informed consent as to whether their PHI is shared and with whom. The ACLU, as we indicate in our written materials, believes that an opt in consent requirement with restrictions is the mechanism that best protects patient privacy as recognized in both [recording unclear]. I think its also important to recognize that the distinctions between an opt in system with restrictions and an opt out system with exclusions as outlined by Sonia and the lawyer for MetroChicago HIE. I think what's really key is, again, that every patient have the ability and opportunity to have an informed consent dialogue about the extent that their information might be shared and with whom. The HIPAA Privacy Rule, again as I outlined in my written testimony, essentially that consent is not required for the disclosure and sharing of information for treatment and payment and healthcare

operations, does not completely answer the questions of what kind of mechanism IL HIE should adopt and that's for several reasons. First, as I'm sure the committee is well aware, HIPAA is a floor and not a ceiling. It recognizes itself and it specifically permits covered entities to seek patient consent. Perhaps most importantly, HIPAA specifically incorporates limits on the sharing of information. That is incorporated in state and federal laws that put restrictions on the sharing of patient information. We've heard testimony today about some of those state and federal laws that restrict the sharing of information without specific patient consent. I won't repeat that testimony. But I think that it's really important for the committee to appreciate the fact that the behavioral health limitations, with respect to HIV/AIDS, the restrictions with respect to sharing of data pertaining to substance abuse treatment. But they're really only the tip of the iceberg, in that there are whole hosts of other areas of sensitive or as the lawyer for MetroChicago termed it HC PHI, that require devising a system that allows the patients great ability to control the granularity of their personal health information, that is available for sharing on an electronic exchange, and some control over who that information is shared with. Just briefly, some of those areas include: the testing that is done pursuant to or that's defined under the Federal Genetic Information Non Discrimination Act (GINA) and the state equivalent the Illinois Genetic Information Privacy Act (GIPA). There are a whole hoax of legal protections and state federal law regarding information about victims of domestic violence or intimate partner violence and sexual assault violence. Those populations, I think, are particularly vulnerable and it its critical to recognize that its only in those instances that the patient can best assess the risk of whether that info should be shared and with whom. I'd also like to point out that there are some very, very important provisions regarding minor healthcare and the need to segregate and segment minor healthcare. There's an entire section in my written remarks that identifies almost a dozen state laws that provide authority for a competent minor to self consent to a wide variety of medical care, including reproductive healthcare, including treatment of sexually transmitted infections, including testing for HIV, including some level of mental health testing and treatment. And it is critical that the minors be permitted a confidential opportunity to decide whether they consent to the inclusion of that information in an electronic exchange. And whether they consent to access to that information by personal representatives name with their parents. They're also a host of injunctive provisions, some of which I've litigated, many of which I've litigated here in Illinois that impose restrictions on the sharing of personally identifying information, for example, whether a woman has had an abortion. Consequently, again as I made clear in my written testimony, a number of states and a number of providers have developed protocol, that's probably where that essentially either eliminates confidential health information from the system entirely, such as the general council that metro described today- basically non-disclosable or non-shareable personal health information. So for example, the state of New York has adopted a system where by it does not include in its electronic exchange medical records for minors between the ages of thirteen to eighteen, except for information regarding allergies and immunizations. Similarly, Kaiser Mid Atlantic providers have adopted a similar protection like that, such that they tag all of this data and essentially don't share. So at this point, I'd just like to reiterate that informed consent option that allows each patient the opportunity to opt in

and impose restrictions on the granularity and sharing of the data would be provision that most protects the confidential patient privacy that I think underlies our entire system of healthcare. It's really important to reiterate that not withstanding the really significant public health and patient health that could be gained with the broad sharing of information. At the end of it all, it's really, quite frankly, the patient's right to control his or her own medical record. That construct really provides the foundation of the entire delivery of medical care unless your culture, as well as the legal constructs that have grown up over the past two thousand years. Going back to the Hippocratic, the Hippocratic bargain that physicians and their patients engage in, really as essentially, the patient tells the physician the most private, intimate details of his or her life. The provider physician guarantees that patient a certain level of privacy that conditions the patient additional consent to examine him or her in intimate ways that would not otherwise be permitted. And that notion of acquiring informed patient consent as a precondition for medical care continues to underline all of our constructs on how that medical care is delivered. So I ask this committee, recommendations for protocol to keep in consideration, that really at the end of the day, we need to be highly sensitive too, and the law is already highly sensitive to the needs for individual patients to be able to control sharing and de-segmentation of their electronic health care information. Thank you very much. I'm glad to answer any questions.

Carl Gunter: *I find this segmentation problem intriguing to be brought up here, which is one would like to take the record and divide it into pieces, so the patients can decide which pieces are shared. So that if they have parts of it that seem very sensitive and they don't think they need to be shared and are willing to share the parts they feel comfortable sharing. On the other hand, there's an enormous technical challenge with this, that if you give some examples of practical ways of doing it, but in many cases it's much harder to see how it would be done, how you would take the record and break it into bits and pieces. I thought for the Illinois Health Information Exchange that probably want some track that allows us to do as much of this as is practical, as it becomes practical. I wondered if you could speak a little bit to- is there an incremental strategy that you can see or that would help us to make that available as it becomes technically feasible and what parts of it you think are technically feasible now.*

Colleen Connell*: I'll give you the caveat that I'm a lawyer not a computer scientist- which I know that's your background, Mr. Gunter- I would actually recommend the two White Papers that the Office of the National Coordinator commissioned George Washington University Department of Health Care Policy. One is on the issue of patient consent options, and the second one is on the issue of granularity, it's entitled Data Segmentation. And both of those White Papers are available online and are sighted in my written testimony. And both provide some guidance as to how a health care exchange could be set up to respect the kinds of granularity I've testified about. And I want to acknowledge that I think it's not easy. To paraphrase Mr. Miller from Central Illinois, I think that some information, some records are better than none. And quite frankly, the notion of a complete health care record is quite frankly, I think a myth. So I think that one could really anticipate that there would be almost a sort of health care*

medical history report card that might include such things as, the obvious, blood type, our age factor, gender, allergies, drug allergies, immunization. You know, that is the kind of information - and again, lawyer not health care provider- that might be most immediately needed, whether in an emergency situation or as a baseline for any care by a specialist or other health care provider. And then allow the patient to segment. For example, reproductive health care, or allow the patient to segment HIV status, or allow the patient to segment a whole host of other information. And quite frankly, I think we've really identified the big ones and they're areas in which stigma attaches as testified by the AIDS Legal Council and I think that goes in the area of reproductive health, like abortion and for minors, contraception. And I think that the other big ones are ones in which the patient is at risk for future violence. The Department of Justice was asked pursuant to the violence Against Women Act to protonate protocol regarding the sharing of forensic record, medical records pertaining to the examinations of women who are domestic violence victims or sexual assault victims. And those protocols, which are also cited in my written reports, underscored the need to allow the patients to impose restrictions on who gets to share that information. But impose pretty strict restrictions on the sharing of that information, even within the health care system, both because of future attacks on the woman and because in particularly small and rural communities, it is highly likely that someone with whom those records are shred, whether in the hospital or subsequent follow up care, might know the victim, the perpetrator, or both. Having grown up in a town of 129, no zeros after that, I can assure you that when you went to the doctor, lawyer or courthouse, people knew who you were and who your family was. My understanding is that the technology does exists to segment that data and I think that you can segment it either by not including it in the change of the first instance and then I think that one of the subsequent, one of the earlier testifiers talked about how you can also perhaps share the data, but not have it be visible. Which I think is something maybe the Public Health community might be able to speak to more knowledgeably than I am in terms of whether their security position.

***Carl Gunter**: Just to follow up, very interesting answer and I think it's intriguing to hear examples, like you gave, of specific things we could probably do. I just wanted to record, this is partly for the committee members, that there are two dangers to the segmentation issue. One of them is if you have too high a bar, too much segmentation, that the people who are involved would be disenfranchised from the system because simply no one will share any part of their record because they don't know how to break the record. This is a concern we've heard repeatedly in front of this committee, that the mental health community doesn't want to be disenfranchised because of the challenge of segmenting the record. We still have to find a way to do it, it's a technical job. The other thing is a dual threat, if there are a lot of people who are vending products in the area now, and the ability to fool patients into believing their record is being segmented is a lot easier than segmenting the record. So we need some evidence that the segmentation is achieving its goals. There's been a long body of research on de-identification, the effects of de-identification and how hard that is, which is essentially segmenting the patient's name from the rest of the record. And I think we need a similarly serious agenda for looking into segmentation and it's effectiveness for other*

cases. So theses ideas, like having the patient doing the segmentation, nice thing to have on the table. I don't know what evidence there is that patients know how to do that, but that's the kind of thing to look into.

***Colleen Connell**: Again, on the White Paper, and I don't remember if it's the one on consent options or data segmentation, the author of the paper talks specifically about the Massachusetts E-Health Collaborative, which is an opt in with restrictions system. And they have 90% patient participation, and they found that in a really meaningful informed consent dialogue does really help patients to avoid, or at least minimize infusion that you talked about that could ultimately lead to patient disenfranchisement. And I think that, putting aside maybe the behavioral health aspects, which I know are very complicated. I've looked at the unbelievable working groups. I think that some of the other areas, in which segmentation would be desirable are probably much easier to wrap one's head around. And I think the risk and the nature of the information is just so much more obvious on a basic person to person common sense dialogue.*

***David Carvalho**: Colleen, this is Dave Carvalho from the Illinois Department of Public Health.*

***Colleen Connell**: Hi Dave.*
***David Carvalho**: Hi. I am participating by webinar, so I don't have access to your written testimony, so I may have misunderstood or misinterpreted a couple of things. So please bear with me. With respect to public health, were you suggesting that the- and you know under current Illinois law, the Department of Public Health has various mandatory reporting requirements that do - look at the tradeoff between patient privacy and public health purposes and legislature is way better the balance made a decision. Are you suggesting those be revisited or that the HIE not be used as the mechanism for complying with those? Or simply that those that are already established by law are fine, but public health purposes beyond that should not be contemplated?*

***Colleen Connell**: Dave, I don't have a global answer to your question. And just, you know for the committee's purposes, Dave and I actually negotiated some of those restrictions by virtue of some injunctive orders that we worked on. I think that, you know, just to talk about, for example, abortion reporting, what's allowed under current law. I think that if you were to require reproductive health care providers to essentially report through the Exchange or make available through the Exchange identifiable medical records that identify by name the women who've had abortions that that would be extremely problematic, from a legal perspective. I think that if one could continue the process that we now have available where by abortion providers report aggregate data on a monthly bases to the Department of Public Health as to how many abortions are performed. I think that, assuming that that data can be de-identified in a way that protects the confidentiality of the individual women, that information might very well be included and available through the Exchange for public health and research purposes. I would just, this goes back to a question that Mr.Gunter asked, I would recommend that the committee might consult Tom Smith, who is the head of the National Opinion Research*

Center down at the University of Chicago, and who I've worked with in a number of different contexts on the challenges of de-identifying data for purposes of making it available for public health purposes while still protecting the confidentiality of the person on who that report is made.

***David Carvalho**: Colleen, I actually, as you say, you and I have worked on the abortion issues, so it's familiar to both of us. I was thinking more broadly. For example, you may know that current law requires the reporting of all cancer diagnosis to the state in an identifiable format, we currently get that and we treat the confidentiality of that very seriously. But the reason why it's identified in an individual format is so that information can be correlated to look at treatment. Similarly, we get reports in various forms relating to infectious diseases, there's a whole list of infectious diseases that are required to be reported for purposes of keeping track of outbreaks in the light. So I think perhaps because you were focused on abortion, maybe I read too much into it, but we at Public Health have been looking to an HIE as a mechanism for continuing to obtain the data that we currently by law are both entitled to and obtain using other platforms. The hoping, especially on the provider end, that having to punch stuff in to seven different vehicles for getting in to public health could be consolidated in to using the HIE. Is that something you've thought about or have an opinion on?*

***Colleen Connell**: I would have to tell you I've thought about it, but don't have a comprehensive opinion. I guess at the end of the day, I think all patients should retain the right to decide whether their medical information is shared, including cancer patients. But I would say that the experience in the states who have opt out with restrictions and the states that have opt in with restrictions, suggest strongly a high rate of inclusion, or opting in to the system, because most people want their medical data shared among their different providers. Many people have, you know, strong desires for public health benefits to be gained from their medical records. And so I think that providing patient consent will probably not be an insurmountable barrier to the high level of compliance that you currently have and that there's a very strong public health bases for, Dave. I will say that in the Data Segmentation White Paper, the authors reference some reports and I believe that they were by Kaiser, in which people reiterated strong public support for public health uses, but still wanted their personal identity protected. So I think that- I hesitate to generalize, having not looked at the raw data, I think that the strong patient support for not having electronic records available to facilitate their health use is also matched by very serious patient concern about their own confidentiality, about their own privacy and what those secondary uses are going to be.*

***David Carvalho**: Why don't you- so we don't take up anymore of the committee's time- Why don't you and I pursue this offline? I value very much the opinion of the ACLU on this topic and I'd like to make sure that it's informed on what it is we currently do; Whether we're talking about changing Illinois law or complying with it through the HIE or continuing to maintain different pipelines. I'd like to make sure that I understand what are your thoughts and you understand what we are currently doing.*

***Colleen Connell**: I'd like to do that. Thank you, Dave.*

***Harry Rhodes:** Colleen, you mentioned the Massachusetts model of opt in with exceptions. I just wanted to point out that I followed that and initially they had a lot lower acceptance rate than of patients choosing not to opt in. And what they actually had to do is go back and retrain the access clerks and registration clerks. After they did that they were able to get a higher response. So I'd like to point out that I think that properly training your staff does make a difference because if the person does communicate the message very clearly then they will likely opt in. Also I think that another challenge that has been proven and shown in a lot of research studies is that health care literacy really plays in to this a whole lot. And you get a lot of people who refuse to opt in, even with exceptions, because they just don't truly understand the situation. And there has actually been cases where states, at the grass roots level, offer health literacy training so that the consumer is more aware of what they're being asked to share and they have a greater success of getting an opt in.*

***Colleen Connell**: I completely agree. I think that's really important.*

***Harry Rhodes**: I just wanted to make those two points because I think that just allowing the consumer to have an opt in with exceptions is not enough. You're going to have to train the health care provider's staff, the uptake staff, the registration staff, and you're also going to have to offer health care literacy training to consumers, as well. When you have all of those, then I think you'll have a higher percentage. But even that, you do have inconsistencies. The consumer may still not understand, the clerk still may not be able to communicate correctly, but I think it will improve participation.*

***Colleen Connell**: I think those are sort of my concerns too. Which is that, I'm trying to sort of imagine- Well, first of all, I want to ask you, are you talking about excluding or opt in with restrictions, opt out with exclusions you said are pretty close to the same thing. Is it just a handful of specific abortion and other reproductive health issues, genetic testing, violence issues, HIV, is it a small number? If I was handed the Form of Consent, and I'm trying to be a patient now, handed this consent form, and on this consent form is a long list of do I want this in, and do I want that out, do I want this is, do I want that out, do I want this shared with this person, this shared with that person… This is the kind of discussion we had at HISPIC a few years ago, so I mean, I was there, I was listening to that. So I'm just trying to sort of understand operationally, how that would work, what the burden (and I don't mean in a bad way 'burden') but just the ability of provider's staff to manage that and work with the patient to help them understand that consent and what they were consenting to. And then, speaking specifically to this health care literacy, a concern about the most vulnerable patients, the patients most, sort of, affected by the issues of health disparities and that sort of thing, being those that are mostly not in the system. From a public health stand point, those are the people we most need to care about.*

Audience Member #1*: Thank you. I think that you are right. It is by large, probably a large handful of areas in medical care that patients would have the strongest desire, in some instances, the strongest need to segment and sequester. But I want to just, sort of, give the general caveat that I'm sure all of you are much more familiar with than I am, which is that a lot of people's attitudes towards health care is conditioned by their culture, their religion, their socioeconomic status. And I think that a health care system writ large that has identified the quality of patient care as one of its primary values has to device a system that allows sensitivity to those individuals' cultural norms to be reflected in all aspects including the sharing of data. And I want to acknowledge I think that that is extremely challenging to deal with, it's challenging from a legal stand point to deal with. But at the end of the day, our law by large, with few exceptions, allows patients the right to consent to the care they want and to refuse to consent to the care they don't want. Even though we, as health care providers or as lawyers, might urge a different option. And I think that we have to be sensitive and the system has to ultimately protect that. And just, you know, a sort of final answer to Mr. Rhodes's question, I think that you are absolutely right and I think this is really where you were going, that to really implement a system that allows for meaningful patient choice and still serve these other purposes will require the intensive careful training of health care staff. But the gain of that, and this has been documented in both the Massachusetts system and the Delaware state system which is an opt out but with exclusions and again has a very high rate of patient participation. The benefit from that is much greater patient engagement in their own health care, including patients with limited literacy- which I agree we need to be particularly concerned about.*

Elissa Bassler*: Can I just ask one really quick follow up question?*

Mary McGinnis*: As they say, your question is standing between you and lunch. With all due respect.*

Elissa Bassler*: It's only a concern with a patient and a health clerk, right? Not a physician, not a trained person. When I make those exclusions, right, I'm actually revealing a lot to that health clerk, so I think that's more of an observation than anything to answer. So, we can have lunch.*

Colleen Connell: *I'll be back after lunch and I'll make the same offer that I made to Mr.Carvalho. My email is probably all over those papers. I'm happy to continue this conversation after lunch, offline, in the office, whenever.*

Mary McGinnis*: Actually, I have one request for public comment, if we may, because our guest has been waiting very patiently. So Mr. Adams, and then we will break for lunch. So again, please take your time, I mean that in all seriousness. And then we'll break for lunch.*

Bob Adams*: Thank you very much. My name is Bob Adams. I'm with NetSmart Technologies. We supply systems to behavioral health substance abuse providers, public*

health organizations and we advocate on their behalf, just to give you a feel for the scope. We have probably about a dozen organizations here in the state of Illinois. We have about twenty million lives being touched by our systems nationwide. We would advocate that committee here undertake every possibility to include behavioral health and substance abuse data in the exchange of information. Our clients and their patients feel they would be best served by being included in the Illinois Health Information Exchange and having their data included in the exchange. They see enormous benefit in terms coordination and care, they see enormous benefit in terms of our research, using that data to improve outcomes across their populations they are serving. Because there are various large disparities in outcomes for patients with similar diagnosis where there are seemingly small standards of care, but where research could cross a large scale of data and could absolutely improve outcomes for the lives of many, many of the patients here in Illinois. We think that one of things that you could do as a committee is to create a uniform consent policy that has uniform nomenclature. Let me just give you a quick example, if a patient decides that they would like to share their medications and it's similarly called 'prescription medicine' or it's similarly called 'drugs', or it's similarly called 'meds', an automated system would have a hard time understanding that those are all three of the same things. So in every place where you're considering granularity of choice, we would suggest that this committee recommend a common uniform nomenclature, in order for the granularity of choice to be executed. And finally, we would second the opinions of the public health folks here to include behavioral health data and substance abuse data in a de-identified and aggregated fashion in order that studies by universities, by researchers, by organizations who are set up around the United States that do behavioral health research could have access to the data and improve outcomes for the patients being treated. We'll submit a more further detailed analysis, but I know I'm standing between you and lunch. I thank the committee for the opportunity to address the committee and for the good work that you're doing, thanks very much.

***Nicholas Panomitros**: Thank you, we're going to meet back here at 2 o'clock. So we'll see everybody back here at 2:00pm.*

VI. Lunch Break (1:00pm-2:00pm)

VII. Testimonies (2:00pm-4:00pm)

Sensitivity of Patient Data: Safeguards for Certain Personal Health Information

Mary McGinnis:

"Good afternoon. I am going to read some written testimony, on behalf two of the Illinois stakeholders that submitted testimony and requested that this testimony be written in to the record. First of all, I would like to present testimony on behalf of Illinois Maternal and Child Health Coalition (IMCHC) and they thank you for the opportunity to provide testimony. IMCHC is a statewide, nonprofit organization that focuses on the promotion and improvement of health outcomes for women, children, and their families through advocacy, education, and community empowerment. For over two decades, we

have fought for affordable, high-quality health care, and would like to present testimony on behalf of our members and their clients and patients.

As a coalition with a vested interest in improving the quality of care for patients across the state of Illinois, we applaud the development and implementation of the Illinois Health Information Exchange. We believe that the increase in coordination and reduction in administrative costs will have tangible benefits for all Illinoisans.

In order to protect a vulnerable population in this new system, we encourage the Exchange Authority to be particularly vigilant in protecting the confidentiality of minors' health records. Current Illinois state law assures minors the right to a wide variety of health services without the consent or knowledge of their parents or legal guardians. Minors across the state can confidentially access mental health treatment, substance abuse treatment, birth control services, HIV testing, sexually transmitted infection treatment, along with a wide array of medical services after a rape or sexual assault.

Minors' ability to access these services confidentially, and to keep their medical history private, is championed by many health professionals and advocates as essential in encouraging young people to access comprehensive health services. The American Medical Association, the American College of Obstetricians and Gynecologists, and the Society for Adolescent Medicine have issued statements asserting that confidential health services, specifically reproductive health services, should be available to minors. Parental involvement and knowledge may deter some minors from accessing the health care they require. In 1998, McHenry County, Illinois mandated parental involvement for minors seeking contraception. In 1999 and 2000, the proportion of births to women under the age of 19 increased while it decreased in nearby counties with similar socioeconomic and ethnic demographics. This aligns with the American Medical Association's finding that less than 20% of teens would seek care related to birth control, sexually transmitted infections, and drug abuse if parental involvement were mandated. Adolescents are simply less likely to access care without the guarantee of confidentiality. Therefore, assuring the privacy of their medical records is critically important.

We hope that you will use the IMCHC as a resource on this issue. If you have additional questions, please contact Kathy Chan, IMCHC's Director of Policy and Advocacy at 312-491-8161x24 or at kchan@ilmaternal.org. Thank you, once again, for your efforts in safeguarding minors' health records in the implementation of the Illinois Health Information Exchange.

Mary McGinnis:

So I believe the members of the committee have copies of this testimony and Ms.Chan's phone number and email address. At this time I would like to also read the testimony of Pamela Sutherland, the Vice President of Public Policy of Planned Parenthood of Illinois (PPIL):

PPIL provides reproductive health care services at seventeen health centers throughout Illinois. Last year we provided 163,261 patient visits. Because of the sensitive nature of many of the health care services we provide, we welcome the opportunity to comment on policies related to data privacy and security for the Illinois Health Information Exchange.

Panel 1: Patient Choice: Options and Permitted Uses for patient Data

Patients need to feel empowered when it comes to accessing health care. If they are denied choices when it comes to controlling their health information, their relationships with medical staff can be diminished. In certain circumstances involving deeply private and personal issues, patients may avoid seeking care if they fear they cannot control who has access to sensitive information as well as how they have access to it. Therefore, patients should be given a choice whether their electronic patient data is transmitted through an HIE. Moreover, they should be afforded choices when it comes to the use of data by clinical treatment professionals. To make it easiest for both patient and provider, the option of opting out (affirmatively declining) of participation in the HIE must be afforded to all patients.

Panel 2: Granularity of Patient Data

On occasion, some patients have met with judgment and even outright disapproval from health care professionals when they have revealed drug use, unconventional sexual behavior, or having has an abortion. These patients have often felt that the treatment they received would have been different and possibly of a higher quality if certain information were not revealed to the provider. Therefore, while we understand that it is best when a provider has all of the information, there may be times when a patient does not want certain health information released. Therefore, patients should have the right to sequester specific elements of their patient record from all or certain providers. In addition, the patient can be given the option of sequestering certain health information or allowing the entire medical record to be accessed in the case of emergency treatment. The decision to sequester certain information must not exclude the patient from participation in the HIE because the benefit of having quick electronic access to most of a patient's record is better than have no access at all. Finally, a patient's data should only be available to medical professionals providing health care to that patient. The patient data should not be open to access by public health authorities. Opening the HIE to access by public health authorities would foster mistrust and unease in many patients.

Panel 3: Sensitivity of Patient Data: Safeguards for Certain Personal Health Information

As stated above, patients often have to reveal highly personal and private information when receiving medical care. The purpose of having special consent procedures for certain health services is to ensure a heightened security for that information and to assure patients that they are "safe" in revealing sensitive information to health care professionals. If patients do not feel "safe" some of them will decline health care putting themselves and possibly others at risk. Therefore, special opt out procedures should be extended to the inclusion of personal health information related to services such as behavioral health and substance abuse. When these health services are

involved, the patient should be given the opportunity to opt out of entering that health information into the HIE or sequestering if from certain providers.

Another issue which is pertinent here is the issue of minors who consent to health care services. In Illinois, minors are guaranteed confidential care without parental consent for certain health services. These services include mental health, substance abuse, testing and treatment for sexually transmitted infections, family planning services, abortion, and pregnancy care. One of the main reasons that the law allows for minors to receive these kinds of health care without parental involvement is because there is a risk that some minors will forgo care and put themselves and possibly others at risk if parents are involved. Because minors are allowed to give consent for certain confidential health services but not all health services, the HIE must have a system set up to allow minor patients to sequester certain personal health information from both specific providers and from their parents or guardians. The minor must be able to sequester information from providers who they do not trust to keep such information confidential. For example, a teen might be concerned that a primary care physician may intentionally or even inadvertently reveal information about birth control use to a parent. Moreover, if the HIE allows parents to access the confidential personal health information of a minor, it would be in violation of numerous Illinois laws which guarantee confidentiality for certain health services.

Panel 5: Patient Choice and Consent: Operational Protocols

We suggest that a good way to inform patients of the risks and benefits of the HIE is provide an informational brochure or pamphlet to patients when they are given the option to completely opt out or sequester data and each time they consent to care for sensitive issues such as substance abuse. The brochure should be easily understandable to someone at a sixth grade reading level. The brochure should include an explanation of a minor's right to privacy for certain types of health care. Providers should designate a staff person who can provide additional explanation if a patient has questions. This person does not have to be the health professional that is directly providing care. Consent can be provided orally as this information sharing is similar to when patients are orally asked if test results or reports should be sent to primary care providers. Consent to participation in the HIE should continue until a patient revokes the consent. It does not need to be renewed.

Panel 6: Patient Choice: Current and Future Technologies

Patients should be given a unique identifier. They should also have access to their own medical records. If they believe there is an inaccuracy, they should not be allowed to unilaterally change the data. Instead, a system should be in place for the patient to contact the provider to correct the data. This will ensure that if a patient does not understand a particular test or report, they will not change something they do not understand.

Panel 7: Protecting Patient Data: Security Compliance Standards for Health Information

Exchanges

As stated above, patients should be assured the utmost privacy and security, particularly when it comes to sensitive health information and minors' access to confidential care. Access to data stored in the HIE should be limited to patients and the health care professionals providing them with health care. If personal patient information is accessible to public health authorities, governmental bodies, or others, patients will not have confidence in the security and privacy of the HIE. Security and privacy standards should be consistent across all HIEs in Illinois to ensure that all patients are provided the same standards and to avoid patient confusion. In order for the HIE to be successful, patients must be willing to participate. If patients do feel that the system is secure and the information they want to be private will be kept private, they will not participate.

Thank you for the opportunity to provide comments on behalf of Planned Parenthood of Illinois.

Mary McGinnis: *So Colleen, we're going to invite you back up to the podium. And I hope you had an enjoyable lunch.*

Colleen Connell:

Thank you again for the opportunity to testify and what I'd like to speak to briefly is the issue of what kind of protocol might be useful in helping to segment sensitive health information. As I set forth, in my written testimony at pages six and seven, the ACLU has a position that the committee should recommend that protocol be developed that helps to segment sensitive patient health care information. That the patient feels desirable to exclude from general access on the registry or feels the need to exclude on the registry. And, very briefly, those protocol include: requiring providers prior to releasing patient names to a registry to advise each patient individually of the opportunity enrolled in the exchange and of the right to consent to that enrollment or that general patient registry, pursuant to the opt-in provisions that we've discussed this morning. Patients should also be advised that they have the right to segment parts of their personal health record, that the patient considers sensitive.

Ms. Bassler, over lunch, I actually had the opportunity to think a little bit about your last comment about whether the segmentation discussion would provide a great deal of information to the records clerk. And I think that, of course the answer is yes, but I think not in such a detailed fashion that the patient's real confidentiality necessarily would be a bridge. I've looked at some consent templates and I think that it's possible to frame the issue such that you sort of say globally, are there areas of your patient records that you would like to segment, if they exist. I realize I'm talking like a lawyer and not something many patients may respond to, but you could list those confidential or sensitive health information areas that we discussed and word it in such a way that the patient wouldn't necessarily disclose that there worse such records in existence only that if there were they would need to be segmented. The other thing I think that warrants discussion is that, given how fractured- and I don't mean that necessarily in a negative way- but given how fractured the delivery of

health care is, such that speaking as a woman, you might have a different OBGYN, you have a different internal medicine person and maybe you have a different dermatologist. I think that much of the segmentation is possible at the provider level in a way that doesn't give sort of a general person or general record clerk much more information other than what is normal in the course of business. And of course those people are acting in the offices of the physician and do have a patient confidentiality obligation themselves. But I think that, just the way that our medical care is delivered will allow some of that segmentation to occur fairly routinely- not without thought, but I think it can be done fairly routinely. Other protocol that I think is really important is the development of protocol that allows patients to revoke consent that they've provided and that allows them to restrict the future sharing of information; Protocol that allows patients to segment any sensitive health information that is covered by law, such that was discussed earlier this morning. And I think that there is, of course, the question that we talked about a little this morning, which is how you deal with confidential health information that's provided by minors, particularly prestigious of the minors who have self consented for. And I think both the testimony of Kathy Chan and the testimony of Pamela Summerfield that Mary read in to the record, emphasized the need to develop protocol to segment those records. And both the White Papers that I referenced earlier this morning provide examples of how that can be done. I think other examples are contained in the footnotes of those discussions. But I think, at the end of the day, it's really imperative for all sorts of good health reasons- including the fact that minors will not seek certain types of healthcare if they feel their confidentiality will be breached- to think about and to incorporate those segmentation requirements in to whatever recommendations the committee makes for the ILHIE. One final area in terms of segmentation that I think is really important to mention specifically is the issue of segmentation with respect to payers, because my reading of The Authorizing Act for ILHIE contemplates payers will have access to certain amounts of data in the system. And so, proceeding with that assumption, the ACLU is of the position that patients must have the ability to restrict the disclosure of PHI to payers. At a minimum, the committee should recommend rules that, one, consistent with the HITECH amendments to HIPAA; allow patients to restrict disclosure to payers of personal health information that is related to treatment or services for which the patient has paid for out of pocket. A second to restriction would be those anticipated by both the Federal Genetic Information Nondiscrimination Act and the Illinois Genetic Information Privacy Act, both of which appear to allow a patient to restrict access to payers. And then finally, I think the committee should contemplate allowing patients to restrict access to payers for all personal health information except for that medical treatment or service for which reimbursement is being sought by the particular payer seeking access to the medical care. I think that the patient's interest in confidentiality demand that there be some time limits placed on what information payers have access to, particularly given the fact that some of those services may have been rendered years or maybe even decades before that particular payer was responsible for reimbursement. I think that I've already discussed at great lengths the special protocol with respects to minors. I don't have any additional prepared remarks, unless someone has questions. And I guess the other two points that I would make, again in reference my prepared testimony, is that the ACLU is of the position that consistent with existing law here in Illinois as well as Federal law, which allows patients to access their medical records that are held by individual providers, that the committee should recommend

protocol that allows patients to both access their records through the exchange and to arrange for correction should there be inaccuracy in that record or should the record need amending. And then finally, the ACLU is of the position that the committee should consider and recommend rules that define what constitutes misuse of data that's in the exchange recognizing that the vast majority of users who access the exchange are accessing for purposes of providing quality health care and helping patients. But I think it's very important that rules be implemented that guard against those few who would use information in the exchange for purposes of discriminating on the bases of providing health care, for profiting or for other gains. So that point, that's pretty much the extent of my prepared testimony, but I'm glad to take any questions.

Audience Member: *The idea of letting patients use the exchange too seems very attractive because we know from testimonies we've seen here and saw that the patients would really like to have some capability of getting access to their own records efficiently. However, it's a major technical requirement. I was wondering how many other state health information exchanges offer that service?*

Colleen Connell*: I'm very sorry; I don't know the answer to that. I think that sort of colloquially from our ACLU affiliate in New York, it seems like the New York exchange might contemplating that. But I can definitely understand the technical challenges of allowing that. But, you know, I might add that lawyer not technical person, certainly some protections of the integrity of the data might be maintained by 'read only' access for patients. And, requiring, as I believe it was Mr. Miller from Central Illinois Exchange who said that they believed in the importance of allowing the correction of errors at the source of the error. I think that people who are actually on the ground in terms of designing and implementing these systems could probably apply on that more knowledgeable than I do. And maybe one of the things might be to have it access through whatever regional exchange [recording unclear]. As I say that, I think that it may contradict the other directive of the statute authorizing ILHIE, which really directs the Authority to contemplate protocol for sharing data across state lines.*

Elissa Bassler*: Yeah, I had a question about what you said about restricting access to payers. And I don't know, under affordable care there's all kinds of things regarding underwriting and things are going to change, and I don't know how that would work. But I do know, that for instance, when I applied for life insurance and I think when you apply for health insurance you actually sign away the right, your insurers can look at your health record. So I'm not sure, I don't know what happens under ACA, on those sort of issues around underwriting and stuff, so maybe it becomes different so this is important. But currently, if you apply for insurance you tell them they can have your record.*

Nicholas Panomitros*: I think what Elissa is trying to say is that you don't really have much negotiation power when you're dealing with life insurance. You either give it up or they're not going to insure you.*

Colleen Connell*: Right, and I think health insurance too. 20m to 37m*

***Mary McGinnis**: Colleen, thank you again for your time and for your testimony today. We're going to move on to Panel 5: Patient Choice Managing Consent.*

***Mark Chudzinski**: Since we're running late I would just like to point out to the committee that there are three, a five page paper and two one page paper, on Panel 5 included in your summary. The issues are, in terms of policy questions are: (1) What is the best way to inform patient choice regarding the risks and benefits of HIEs? (2) Should providers have to discuss HIEs with patients such that "meaningful choice" is obtained? Or do "Notice of Privacy Practices" accompanied by informative website disclosures suffice? (3) Should all consents be written or can consent be obtained orally? (4) Once consent is validly obtained, is it valid for an unlimited duration of time? Or can it be revoked after a certain amount of time? (5) If consent can be revoked how should providers reconcile conflicting patient consents? With regards to the OHIT responses to recent requests from ONC, we have indicated that revocation is reasonable. We however have suggested that with regards to duration of consent that is challenging as well as providing meaningful choice that is also challenging. With that, I'll hand it over to my colleague, Mary McGinnis.*

***Mary McGinnis**: Good afternoon. I believe we are expecting participation from Mr. Mike Berry on the phone. Mike, are you available?*

***Mike Berry**: Hello, can you hear me?*
***Mary McGinnis**: Yes, we can. Thank you.*
***Mike Berry**: I'm sorry; did you say you can hear me?*
***Mary McGinnis**: Yes, we can. Please go ahead.*

***Mike Berry**: Okay, I'll go ahead with my testimony:*
[Below is Mr. Berry's submitted written testimony]

Good afternoon, Mr. Chairman and members of the committee. I am Michael Berry, Project Manager for HLN Consulting, LLC, a health information technology company based in San Diego. I have been with for HLN for over ten years, building immunization registries to connect providers to public health, connecting public health to health information exchange, and assisting HIEs with privacy and consent policy and technology. I have contributed to the Health Information Security and Privacy Collaborative and other ONC efforts related to privacy and security. And I am currently engaged with OHIT, in collaboration with the SHARPS project at the University of Illinois – to define a technical architecture and develop a prototype for a privacy and consent layer within the Illinois HIE.

I would like to thank you for the opportunity to provide testimony today regarding the operational aspects of obtaining and managing consent in an HIE; specifically, regarding different strategies being used in HIEs around the country.

First let me make the distinction between 'push' messaging, such as the Direct messaging in ILHIE Phase 1, and 'pull' messaging, such as the aggregated query-response in ILHIE Phase 2. The consent strategies I'm discussing today are generally limited to the 'pull' model – many HIEs offer both a push service such as results delivery, and a pull service for on-demand query-response; and it's typical for the results delivery component to have no consent function, and the query service to have one.

As you know, broadly speaking there are a number of high-level consent models that an HIE may choose to implement. These range from no consent, to opt-out, opt-out with exceptions, to opt-in, and opt-in with restrictions; or a combination of these models. The selection of a consent model is typically influenced by federal and state law, HIE policy, as well as the input of stakeholders – providers, patients, public health, and others.

That consent model decision impacts the operational requirements for obtaining and managing consent. For example, the expected volume of consent requests in an opt-out HIE may be lower than that of an opt-in HIE. An opt-in system is more likely to benefit from a consent collection mechanism that works in real-time and is integrated into the patient encounter; as opposed to an asynchronous, offline process developed for an opt-out system. A partial or hybrid consent model will require more information in the opt-in or opt-out transaction, potentially requiring additional patient education efforts and more complex systems to manage the consent data that is collected.

HIEs today collect consent preferences from patients using a number of methods which can be categorized into two groups: directly from the patient to HIE, and indirectly through the patient's provider.

- The primary advantages of the indirect method, through the patient's provider, are that the HIE can rely on the provider to identify and authenticate the patient, and that the consent action can be integrated into the patient encounter.

- The primary advantages of the direct method are less burden on the providers – who are not always able to absorb the added time and cost of collecting consent – and potentially more control in the hands of patients.

In both methods, the consent is collected from the patient (or the patient's authorized agent) either electronically (such as on a web-based form), on paper, or orally (which may be in person, or over the telephone).

When the HIE is collecting the consent directly, a key challenge is to identify the patient and to authenticate the consent – to be sure that the consent is coming from the patient or from someone authorized to provide consent on behalf of the patient. This can be difficult. The same name-matching challenges that HIEs encounter when exchanging data with providers are present in accepting consent directly from patients. Regarding authentication, the required level of assurance is a policy question for the HIE, and it may be influenced by the consent model that has been chosen. We have encountered examples in other states ranging from an opt-out web form that only requires basic demographic information (name, address, DOB, phone); to a paper opt-out form that requires the demographic information plus a signature by a state-licensed health care provider or a notary public stamp; to a web-based opt-in form that requires demographic information plus a component of the patient's Social Security number. We are also aware of commercial vendors that market patient identity proofing services to HIEs, where the web form is supplemented by a series of questions derived from the patient's credit report. Another option is to require a token – such as a PIN number – obtained from patient's provider. Clearly, there is a trade-off between the level of assurance and the patient's convenience.

When the provider is collecting consent, there are a few key decision points: First, the consent can be a provider-by-provider consent or a global HIE (multi-provider) consent. Second, the consent can be stored by the provider only, or sent to the HIE; generally, a multi-provider consent requires that the consent be transmitted to the HIE. And third, the consent can be solely an assertion by the provider – the provider asserts that the patient consented – or it can contain some token from the patient such as a signature on paper or an electronic signature captured in the provider office.

It's also worth noting that in the opt-out model, some HIEs – in order to better ensure informed consent – adopt an "opt-out with notice" policy, where all patients receive notice (either through the provider or directly from the HIE) of their record going in to the HIE and of the opt-out policies and procedures that will apply.

Once the consent has been collected and stored – either at the provider's office or at the HIE – the HIE needs to provide a way for the patient to change it. In the opt-out model with an opt-out form, typically there is a companion opt-out reversal form. In the opt-in model with an opt-in form, typically a patient can simply submit a new form to update the existing preferences. To move beyond that level of complexity – to allow a patient to view his or her current consent preferences, and update them – generally requires a web-based patient portal, with the higher level of patient identity assurance and authentication requirements that go along with that. Many commercial HIE vendors offer patient portal products, though the implementation of these products in state HIEs is still in its early phases.

What about granular preferences? I mentioned earlier that a partial or hybrid consent model will require more information in the opt-in or opt-out transaction and make it more complex. It's important to note that many state HIEs have incremental deployment strategies that include a less ambitious initial phase – such as an all-or-nothing consent approach, a static set of information sources and purpose of use, an unlimited duration of consent – followed by more ambitious future phases. So as we look around the country we do not currently see a lot of granular preferences being offered to patients in their opt-in or opt-out forms, but that doesn't necessarily reflect the changes under development as HIEs strive to ensure meaningful choice for patients. In one state we are aware of, the opt-in form allows patients to select individual provider organizations who will be allowed to access the patient's record, or to limit the purpose of use to emergencies. In a pilot project in another state, the opt-in form was required to be signed at each provider organization, and it authorized data only from that organization into the HIE.

In conclusion, the operational requirements of obtaining and managing consent in an HIE are influenced by the consent model selected by the HIE; and once the consent model has been chosen there are important tradeoffs to consider in terms of collecting the consent, storing and transmitting the consent, and updating the consent.

Mr. Chairman and members of the committee, thank you for giving me the opportunity to speak to you today.

***Mike Berry**: Does anybody have any question? I'd be happy to answer them.*

***Carl Gunter**: Hi Mr. Berry, this is Carl Gunter speaking. I was wondering if there exists a record of the states with the options along the lines you chose, that you describe there, where we could, say, see a spreadsheet and see which thing each given state had. I know that there are some things like this for certain kinds of sharing information that had been developed by Joe Pritz and others. I was wondering for this consent options thing if there was a spreadsheet for that somewhere.*

***Mike Berry:** So you mentioned the Joe Pritz report. So, the data that I drew in order to write up the testimony came from a few sources, so I'll walk through them. First, was essentially my personal experience in places like Vermont, Rhode Island and with HISPIC and with the Upper Midwest State Health Policy Consortium, the ONC, the George Washington University, the Joe Pritz, Privacy and Security White Paper that you mentioned. That had a survey of Delaware, Indiana, Maryland, Massachusetts, New York, Rhode Island, Washington, Virginia and Tennessee. That document now is almost two years old, but has a lot of good*

information in it. I would say that's the closest thing to what you're asking about. That report has an appendix in it with a table of those states. Upper Midwest State Health Policy Consortium has a draft report- I don't think it's been officially released yet- that has some information on Minnesota, North Dakota, South Dakota, Wisconsin, and of course, Illinois. And there are a couple of vendor White Papers out there. But the answer to your question potentially is aside from the ONC White Paper that had, what nine or ten states in it, there is no table out there, currently, that has a survey of all states.

***Carl Gunter**: Thank you.*

***Mary McGinnis**: Any other questions for Mike Berry? Thank you very much, Mike. We appreciate your testimony. I'm wondering if we have Dr. Steven Spool on the line.*

***Cory Verblen**: Mary, I don't believe that he is.*

***Mary McGinnis**: I think because we are running a little bit behind schedule, we have missed some practitioners throughout the course of the day. And again, in the interest of time, I do have some additional testimonies that I would like to read in to the record. However, I'm going to defer that temporarily so that we can move to Panel 6: Patient Choice and Identity Management. I believe Mark has some opening remarks.*

***Mark Chudzinski**: For Panel 6 I'll simply read the four principle questions involved with this panel. (1) Should the state-level ILHIE utilize a unique patient identifier for the purpose of matching patient records? (2)To what extent should the state-level ILHIE impose upon providers connected to the state-level ILHIE standards for the degree of patient matching accuracy achieved in provider systems? (3) Should patients be able to access their data transmitted through the ILHIE to check for inaccuracies? (4)If inaccuracies are apparent, should the ILHIE address patient requests to correct data or refer such requests to the patient's healthcare providers?*

***Mary McGinnis**: Thank you, Mark. I'd like to welcome Dr. David Stumpf to the podium and I believe that we have **Dr. Barry Heib** on the phone as well.*

Dr. David Stumpf:

Thank you very much for the opportunity to address the committee. I'd like to start by commending the committee and the staff for doing an excellent job of formulating the problem statement we're dealing with here today.

I am David Stumpf, I am a licensed physician in Illinois. I'm also a consultant to ILHIE. I'm here today on behalf Global Patient Identifiers, one of my consulting operations. I have no financial interest in them. I only get paid for expenses, if I travel for them- nothing else. Dr. Barry Hieb is one of the executives at GPII and he is on the phone to serve as back up for some technical issues I may be a little deficient on.

There are kind of two high level things I'd like to communicate today. One is the current state of patient identification and what the solution we proposed would bring to the table and also how it can be used to segment by privacy classes. Our testimony isn't going to

address your specific privacy policies, per say, but really some of the infrastructure that's necessary for accurately identifying patients. The problem that we're trying to solve is the fact that best of breeds systems today, using matching methods, demographics, patient identifiers and hospitals, so on, is the three sigma level. I have personal experience with this, having worked for six years at United Health Group, which I think has really best of breeds systems. And three sigma is certainly satisfactory for paying the claims. But what that means in an open system environment is that you're going to be making thousands of errors a day, if you're doing millions of transactions a day and misidentifying patients. And that's an unacceptable performance. We really need to be at six sigma level.

The solution we're suggesting is based on a set of standards which are outlined in the bullet points on the first page of my testimony. Their ASTM/ANSI standards, they've been enhanced by this particular vendor. The Global Patient Identifiers to also incorporate privacy classes and privacy classes allow you to issue an entirely distinct identifier for purposes of managing protected information. Just like you have two credit cards in your wallet, you may have two patient identifiers with different privacy classes, which allows you to manage a lot of the complexities.

I would point out, that on the first page, those bullets are really specifically designed be sequential. So you don't have to buy this whole package all at once. You can look at the first four bullets as being internal to the ILHIE solution. You can implement those in a sequential manner or any of those involving anybody outside of the ILHIE. And I have talked to the vendor here, InterSystems, and they can certainly do this if requested. Certainly, ILHIE has to adopt some kind of internal identifier for its own use- to which a lot of other things can get matched. So why not go with a national standard for that purpose. And then one can begin to add on some of the other bullet points depending on the policies and procedures you adopt, including making it available to other providers to be used and etc. I won't read all of those specifically, in the interest of time.

So, I think the other general point is that, you know, identification solutions must promote not only information, but protect privacy. You have to do both of them simultaneously. One is not exclusive of the other one and this solution of using a unique patient identifier based on a national standard would address this issue. I would also point out some of the other issues raised here about patient access to their data. These unique identifiers will allow them to do that too, along with other things, like biometrics or pins that are issued by the provider itself. This solution has actually received quite a lot of attention. The VA is using this solution already. They've saved 8 million dollars with the ability to avoid the problems duplicate records and merge records. The cost of that is really staggering. In a single health care system in Southern California, actually employees twelve people to manage the ambiguity of patient identification within their system. And even then, they haven't got it right. There report, which is referenced, really says the only way to solve this is to have a unique patient identifier. So that's what we're here to advocate for and to suggest a specific solution. I'd be very open to any questions. Thank you.

***Audience Member**: I know that under HIPAA- when HIPAA was first introduced, it's been a long time ago- they included the patient identifier and that was the only one in which rules were never released, you can propose rules. And I'd just like to understand, because the barriers that were identified were really the patient privacy and confidentiality. How that has*

changed now versus then and what would make- besides the clinical and efficiency argument, what are the barriers that have been overcome?

Dr. David Stumpf: *That's an excellent question. We're in a conundrum right now because HIPAA mandates, actually mandates that we have a unique patient identifier and then Congress came along and said not with our dime, not with allocated funds. So it does open the door to other paying mechanisms, how to pay for this, either at the state level or through private funds, or whatever, so we're really not prohibited from doing this. The principle reason Congress did what they did, of course, was because of comments on privacy from a private community that was concerned that a patient identifier would enhance the ability to steal your identity. The fact is, I think most of us have, you know, had a call from our credit card company asking did you just buy $10,000 worth of whatever. And having a unique identifier is actually a better way to mitigate those risks. You know, there's an interesting report that came out a few years ago from the Department of Justice, the Department of Civil Rights and HHS, looking in to the problem of medical identity theft and it's an incredibly difficult problem when it happens. The only way to really effectively deal with it, is to cut it off at the past or to have an identifier which allows you to locate the records that have been adulterated. Because the problem the patient has, is that they often learn of this by a collection agency coming to garnishee their pay or put a lien on their house because expenses have been run up in their name and they didn't even know it happened. And then, they have trouble finding where are these records that have adulterated my record. Having a unique patient identifier and one of the things that BUHIE does, and I don't think I explained that quite clearly, is that they do not know whose identity is attached to the patient, that's done by the agency to which it's issued. In this case it's be ILHIE, which would manage this pool of identifiers for Illinois population. What they know is who they were issued to and who has used them. So that if the patient happens to be in Florida or Missouri, they would be able to point the requesting entity to the site where those were used that are outside the sphere of influence of ILHIE, itself. So, we think that this is a solution, you know, that is necessary to mitigate a lot of the concerns of the privacy community.*

Mary McGinnis*: Thank you, gentlemen. At this time I'm going to back track ever so slightly. In the interest of time, earlier today, I did not read testimony from Illinois State Medical Society (ISMS). All of the members of the committee do have the testimony from the Illinois State Medical Society in their packets. None the less, I am going to go over their comments are brief and important. So, I'm going to go ahead now and read them in to the record:*

The Illinois State Medical Society (ISMS) is grateful to the Illinois Health Information Exchange Authority for hosting this meeting to obtain stakeholder input on possible privacy, security, and consent management policies for the Illinois Health Information Exchange (ILHIE). Our comments will pertain to Panel 1 - Patient Choice: Options and Permitted Uses for Patient Data; and Panel 5 - Patient Choice and Consent: Operational Protocols.

The development of a health information exchange (HIE) in Illinois has the potential to improve the quality of care by providing physicians and other health care professionals with accurate and complete patient clinical information. The possible uses and benefits of an HIE include the ability of an HIE to compile a virtual patient record that aggregates clinical

information into a single patient record as well as the secure delivery of hospital discharge summaries, consultation notes, and referrals. There will undoubtedly be other uses for the HIE such as providing population analytics that health professionals may need as they take on more risk due to changing reimbursement methodologies.

To be successful, the HIE must ensure the secure delivery of information without placing additional administrative burdens on physicians and other providers. We are concerned that federal guidance to date may add to the administrative burdens placed on health care professionals as the provisions go beyond what the Health Insurance Portability and Accountability Act (HIPAA) require. We cannot support new regulatory requirements that have the potential to place a significant administrative burden on physician practices, especially when a clear justification for the new regulations is lacking.

Panel 1 - Patient Choice: Options and Permitted Uses for Patent Data

Our concerns primarily relate to the Office of the National Coordinator's March 23, 2012 Program Information Notice 003, which would result in additional burdensome administrative requirements placed on physician practices. Currently, HIPAA governs how health care information can be used and shared and is specific on the permitted uses of patient data. It is unclear why the HIPAA Privacy and Security Rule is not sufficient to govern the transmission of patient data through an HIE. The sharing of patient records for purposes of treatment, payment, and health care operations is governed by HIPAA and this should be sufficient for HIE operations. It is unclear why the mode of secure data transmission would lead to more granular choice or why patients should be given a choice to affirmatively consent for exchange of their data through an HIE. The current security practices regarding disclosure should be sufficient for any HIE data exchange.

However, if the HIE uses data beyond the treatment, payment, and health care operations exception, then it should be incumbent upon the HIE to obtain any additionally required patient consent. Panel 5 - Patient Choice and Consent: Operational Protocols

Similar to our comments regarding Panel 1, our concerns with patient choice and consent as outlined in PIN 003, would place undue burdens on physicians and other health professionals in an attempt to obtain "meaningful choice." Again, we are concerned about why the ONC would propose a standard that goes beyond HIPAA simply because protected health information data is being exchanged via an HIE. The current notice of privacy practices should be sufficient to cover data exchanges for treatment, payment, and health care operations via an HIE. It is the responsibility of the HIE to provide a secure environment to exchange data, and such exchange falls within the HIPAA treatment, payment, and health care operations exception. Therefore, we do not see a need to collect additional consents or obtain "meaningful choice." If ONC insists on additional administrative burdens pertaining to patient consent, we would suggest that any patient preferences and consent be obtained via an HIE portal. However, if a patient has restricted the release of data, such a summary of care record should be flagged to indicate that the record is incomplete so those viewing the record will know that they may not be viewing a complete record. An incomplete record can endanger patients.

In summary, the ISMS shares many of the same concerns expressed in the June 26, 2012 ILHIE comment letter on the Nationwide Health Information Network: Conditions for Trusted Exchange. We compliment the ILHIE Authority on its well-researched and articulate

comments. While we recognize the need to ensure the privacy and security of health information when it is exchanged via an HIE, the current HIPAA regulations provide sufficient guidance and any additional restrictions should be justified and balanced against cost and other considerations as stated in the June 26, 2012 ILHIE Authority comment letter to the Office of the National Coordinator for Health Information Technology.

***Mary McGinnis**: We're making progress. I believe we may be approaching the final panel, which is a combination of Panels 4 and 7: Security Compliance for HIEs. I'm pleased to invite John Ceran, an OHIT intern, to the podium.*

***John Ceran**: Thank you. So the committee should have a copy of my paper I submitted, seventeen pages, but I'll give you the quick overview through my presentation. So, with this combination panels there are two central questions: How do we foster public trust in an HIE and then, second, how do we protect the issue of data? So the agenda, first we'll talk- I'll just briefly talk about Illinois law regarding the privacy and security of PHI and then also, next will be the federal HIPAA privacy enforcement. The third topic will be Texas, who will be instituting a bill effective September, 2012, making their privacy security more strict. And then last, we came up with a few proposals.*

So, OHIT completed a comprehensive review of state law and we built a very long matrix, but this is just a short sample. The most strict is the identity theft statute, as you can see it starts with a Class D Felony and goes up from there. That second column is private action to recover damages for the person affected and harmed by the crime. And then on the last column, is the authority, which in this case is the Attorney General. But then when you look specifically to PHI in Illinois, you start with Illinois Medical Patient Rights Act. It's also referenced in the Hospital Licensing Act, but again, the penalties here are thousand dollar fine, Class A misdemeanor- it's not very large. It might not be a great incentive for state attorney generals and D.A.s to bring suits. It's also referenced in the Medical Practice Act, so this would be for a physician. It would be a civil penalty and would be governed by the IDFPR, they would have to take administrative action against their license and the fine would be $10,000. So then moving to federal law- the next slide.

So we've already talked about HIPAA, they're our privacy and security rules. HHS, the Office of Civil Rights enforces those rules. They receive complaints and courts through the breach of identification rule and so they have discretion to do two things: they can take administrative civil action or they can decide to refer those complaints to the Department of Justice, who will take criminal prosecutions. There was a presentation done at the age L.A. a few months ago, where someone from the OCR gave some statistics. So between September 2009 and April, 30, 2012 there were 421 reports nationally involving a breach of PHI for over 500 individuals. There were 57,000 reports for under 500 individuals. Now, that's for the entire nation, but Illinois is the fifth most populated state. We definitely comprise a significant proportion of those breaches. And we're completely relying on the feds to enforce this. There is some state authority, which I will reference later, to enforce HIPAA privacy and security rules. But like I said, we're completely relying on the feds.

So, when I was talking about how they can take administrative action against- or OCR can take administrative action against covered entities, this is a table of the civil violations. And it's a tiered system, so the penalties are lower for when a breach occurs and they don't

have the knowledge and they weren't able to do anything about it. And then you've got the most strict penalties for, let's say they were negligent and when they found out about it, did not correct it. Now, a lot of times you see in the news, OCR settles with covered entity for 1.5 million, that's because that's the maximum bound for when you have multiple violations with an account or it can just mean, it could go on for a week or something like that. And each day it's considered a violation. So if you go to the next slide, it'll talk about the criminal.

So, let's say OCR gets a complaint and they forego doing administrative process they just send it in to the DOJ, who decides to take criminal action. Again, there's a minimum under $50,000, under a year imprisonment and then if you have the intent to sell or cause harm to someone that's when it's the most strict is with $250,00 per violation with a maximum prison sentence of ten years. So these are compared to the Illinois civil and criminal violations.

So, as I was referring to earlier, OCR enforces the rules. But there are, recently with the HITECH Act, it gave the state attorney generals and the states authority to bring civil actions against covered entities on behalf of state residents. And this would be to recover damages for the state residents. Now, before the state attorney general actually initiates one of these actions, they have to serve OCR and effectively get permission from them in order to initiate this action. There's also, they also make the state attorney generals go through training. I reached out to the Attorney General's Office in Illinois, they did have someone who did go through training has since left, the next person is going to do that, so we'll have one attorney general who'll have that training in Illinois.

So we're looking for examples of other states sharpening their enforcing mechanisms to kind of close this gap between state and federal enforcement. And we happened upon Texas, who, they passed a bill in, I think, 2009, 2010 and it becomes effective September 1st. Now, a lot of these enumerated issued are things here were kind of the base for a lot of the proposals we come up with. One important thing added to our consumer website, which provides consumer's contact information for all the relevant agencies that are enforcing the privacy and security rules. In Texas, they increased their civil penalties, they also increased their criminal penalties from a misdemeanor to a felony. They also, as I mentioned, they increased civil penalty range from $5,000 to $250,000 per violation- which is more, actually closer to HIPAA's. They also provide for better cooperation between the licensing agencies, so that if you could get a quick criminal conviction, you could then lead to the revocation of a license, which is arguably, has a greater affect on the health professional's career than an actual fine. It also provides incentive for state attorney generals, if you dangle a bounty in front of state attorney generals, in terms of, if they recover on behalf of residents, they get to keep a certain percentage of it, it'll definitely motivate them. There's an audit system where they're able to essentially stick HHS on covered entities. It's just a way to report them. They require all covered entities to submit their Certification of Policies to an agency in Texas that actually certifies their policies, that they're compliant. It's also, they require breach notifications similar to the federal rule, it's just so the state can be aware of, if there are breaches going on. Like I said earlier, they increased the criminal penalties as well.

So, we logged our proposals into four main topics, and this would be to help build trust in the HIE and also protect patient data: (1) Monitoring, and instituting monitoring systems, (2)Enforcement Strategies, (3)Breach Mitigation, (4) Public Education.

So, first monitoring, you would want to institute a breach reporting rule somewhere to the federal one. It would require all breach entities upon discovery to notify the state and the ILHIE. We also will allow members of the public and patients to actually whistleblow on covered entities when they find out that their data has been breached and possibly provide some sort of financial incentive. Second, provide some sort of technical infrastructure within the HIE to allow for real-time network monitoring of privacy and security breaches. This would be more of an admin control. And then, the third thing would be an audit team function, where either the ILHIE will be sending out teams of auditors to covered entities to make sure those covered entities are compliant. Or you might have a third party self-certification, something like that. I know Texas does it a little differently, where they just kind of refer covered entities to HHS- that could be another possibility.

So with enforcement strategies, we would first start with the appointment of the ILHIE Chief Privacy and Security Officer. This person will be in charge overseeing and managing all enforcement activities for the agencies. There would be a budget for enforcement activities, and possibly incentives for inter-agency cooperation. They would review all complaints that would come in through the breach verification and then they would decide whether or not to pursue civil action and refer it to other agencies such as, IDFPR for physician licensure, or refer to the attorney general for criminal prosecution. They would also be in charge of, once a breach actually occurs, they would kind of direct and manage the mitigation strategy, which I'll talk about later. And then also, they would oversee the public education about enforcement and compliance, privacy rule, stuff like that. All of this is definitely going to require interagency coordination working with, like I referred to earlier, Attorney Generals, Office of Inspector General, Health and Family Services and County State Attorneys, IDFPR, and basically any of the agencies that regulate health professionals and covered entities.

So, as I referred to the ILHIE Privacy and Security Officer, he or she would have civil or criminal tools. For civil, it would refer to licensing agencies responsible for taking disciplinary actions against each covered entity or the departments that enforce the statutes that bring along civil penalties. We also, this slide shows the breakdown of sample increased state penalties that could be instituted in Illinois, you would just put it in one act and all the other acts could refer to this. So you could harmonize it through all of the Illinois state laws. And you'd carry a Class A Misdemeanor minimum, so that it would not carry that blocked down of a felony if it was really something they had no control over. But then you would want to increase those penalties for neglect, for reckless disregard, for fraud or for sale- if your intent was to sell it or to harm the individual, obviously you'd want to bring about the full or harshest penalties. And these ranges were meant to kind of definitely close that gap between state and the federal penalties. And you see below, I have the federal ranges below the sample increased state penalties.

So the next proposal would be breach mitigation. So, as soon as covered entity is reported to a chief privacy officer, that officer would then require the covered entity to come up with a Corrective Action Plan. This would definitely heighten the review and the revision of all of their policies, substantial training for the staff, there would have to be a monitor there to report back to the ILHIE on the changes in those policies, the training and the ongoing compliance efforts would require some kind of biannual formal report. And then most importantly, you would need to have some money for the harmed individuals. And that

would be through the ILHIE Chief Privacy Officer kind of helping that covered entity either purchase insurance or set aside some kind of damage fund to compensate for that harm.

And then finally, public education. I don't know if you've been to OCR's website, they have enforcement highlights, where they kind of detail 'this is the number of reports received', 'this is the actions we've taken', 'this is the money we've covered', it's very detailed and it's something that would definitely foster trust in the HIE. There could be quarterly webinars on enforcement actions, you could even make it mandatory, you know, once a year for covered entities to take part in. And then we would want, to kind of, initiate some sort of outreach program through non-profit organizations for public education we could provide grant money as incentives for that. Thanks.

Mary McGinnis: *Thank you, John. Are there any questions for John?*

Audience Member: I can see the local presence but I think there is probably some efficiencies of doing it at the national level. You know, local level you have efficiencies with the patients as well as some other issues. But one of the questions I had is, many organizations now are crossing the state boundaries and becoming national organizations, and so when you bring and issue before an organization because they incorporated and it may be out of state, where does that fall?

John Ceran*: For interstate issues, you would have to rely on the feds for that. But, I think for interstate issues, depending if there's federal law books, or they may apply to the state law-*

Mark Chudzinski*: If an organization is doing business in the state of Illinois it has to actually register to do business in the state of Illinois. And the state of Illinois would have an interest in protecting the local residents, the patients here in the state. But obviously with many provider and other organizations being regional or even national in character, I would think that there would be a role for coordinating with our counterparts from other states and with the federal government. The question is, do we leave all of this enforcement activity only to the feds, or do we actually put our fingers in this as well in order to assure for Illinois residents the fact that the ILHIE Authority will be their PHI cop, their representatives to help protect data privacy here in this state.*

Audience Member: Just one more question, sorry. You know, looking at the volume, especially the ones that are under 500 individuals, 57,000 cases, I mean, the minimum you're going to be dealing with over a thousand cases in a year, especially as this information gets out there. Do they all require investigation to the fullest extent or is there a modified approach?

John Ceran*: I think, I mean they definitely look in to every complaint. I think I briefly saw something that they take action in 50% of those in Illinois, but I wasn't able to actually find some kind of number.*

Mark Chudzinski*: They have not- OCR has not yet given the details of those 57,000 cases. However, I have heard from speaking to representatives of that agency, that actually a large*

number of these complaints are very de minimus. They might involve somebody misdirecting a fax, and that's a reportable condition if they're unable to retrieve or destroy that fax. And there are other reported cases where it arises from a domestic dispute between a physician and a wife in a divorce proceeding who raises all kinds of allegations. So, there are a number of incidents that may be actual incidents but don't really affect the greater public to the extent some of these other breaches would require investigation by the authority.

***Audience Member**: The HITECH rules and requirements do say that there has to be a risk of harm assessment, so there is an initial investigation whether or not it actually goes anywhere. Each one of them does get investigated and determined if a risk of harm is natural or reputational or another type of harm has occurred.*

***John Ceran**: But I'm sure that federal law for risk of harm is higher than it would be for state. So, I'm sure there's a lot more that we could enforce.*

***Mary McGinnis**: Thank you, John. And I would like to welcome Mr.Vic Bansal from Deloitte to the podium.*

***Vic Bansal**: Thank you, Mary. [Below is Deloittes's submitted written testimony]*

Good Afternoon Director and members of the Committee. Thank you for allowing Deloitte[1] this opportunity to provide testimony on ways to better protect patient data and instill confidence on the use of the exchange. I am going to discuss patient data protection and assuring security compliance to for Health Information Exchanges (HIEs). Needless to say, building patient trust is a "table stake" to realizing the full potential of HIEs. You asked the following three questions related to security compliance standards which are included in my testimony:

1. To build trust by protecting patient data, what restrictions should there be on permitted uses of data by HIEs?

   We believe that building trust comes from a consistent track record; all that it takes is one breach, even of a small scale, to impact trust. There are a few elements to building and maintaining that trust:

   - Implement a broad security and privacy risk management program, including a structured risk assessment, to identify threats and countermeasures for the use of data; doing a risk assessment periodically and publishing the high level results helps in building trust.
   - Provide easy and secure information to patients about their privacy rights and how their information can and will be used through the use of technology tools such as identity and access management (IAM). IAM is the set of business processes, information, and technology for managing and using digital identities
   - Information should be made available on a "need to know" basis and using roles to provide access with robust audit trail capabilities
   - Consent management is a system or set of policies for allowing patients to determine who they allow viewing access to their health information. In the absence of a single state consent policy, exchanges will need accommodate multiple consent models
   - Adopt clear privacy procedures and train employees so that they understand the privacy procedures and designate an individual to be responsible for determining that the privacy procedures are adopted and followed

The Federal Department of Health and Human Services (HHS) has established a breach notification process with the intent of elevating the citizen trust through regulations requiring mandatory notification procedures. As part of the security program, implement policy, process, technology

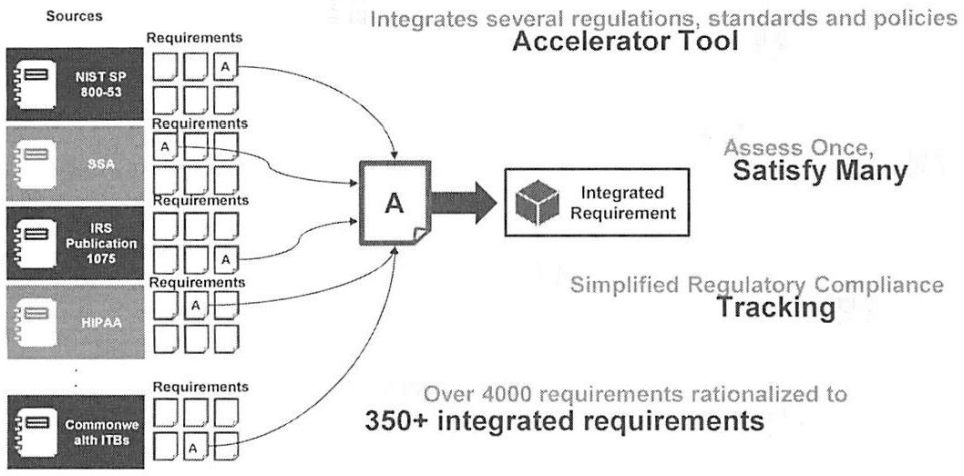
and people changes in the organization to create the cyber awareness and compliance with the mandatory requirements.

2. Which entity or entities should establish and impose security compliance standards on HIEs?

The Office of Health Information and Technology should provide overall governance in establishing and enforcing the security compliance standards on HIEs. OHIT directs the State's HIE implementation efforts and is the custodian for developing a state-level HIE which includes representation from hospitals and universities, businesses, Federally Qualified Health Centers (FQHCs), physicians, nursing homes, insurers, advocates, pharmacies, rural health providers, legislators, the City of Chicago Public Health department, state agencies and the Governor's Office.

One possible approach for establishing security compliance standards and providing a mechanism for continuous monitoring involves using an integrated security regulatory risk framework that rationalizes industry standards, policies, and state and federal laws or regulations. The security risk framework will enable OHIT to assess and prioritize security, privacy and compliance risks, then identify the appropriate risk response strategy, such as mitigating risk through appropriate controls, risk transfer and accepting risk.

The security risk framework can be used to conduct periodic risk assessments on IT assets and processes, select treatment options, monitor the effectiveness of mitigation techniques, and support annual reporting for Federal and State compliance requirements. Figure 1 below illustrates an approach to develop the risk framework.



The integrated security regulatory risk framework rationalization of individual requirements from more than 160 industry regulations and standards and can incorporate applicable security policies, and state and federal regulations. The security risk framework will help enable the State to assess and prioritize security, privacy and compliance risks, then help identify the appropriate risk response strategy, such as mitigating risk through appropriate controls, risk transfer and accepting risk.

3. Should Illinois Health Information Exchange (ILHIE) impose such standards on sub-State HIEs?

   ILHIE should collaborate with sub-State HIEs to enforce the standards by providing them the necessary tools and processes to do so.

   The security program of ILHIE should include sub-state HIEs. Given that the overall exchange and patient data is only as secure as the weakest link in the complex HIEs, we believe that ILHIE may consider not only providing guidance, standards and tools, but also helping to monitor compliance of these sub-HIEs. Utilizing the security risk framework described above could be once such approach.

   By providing an online portal using tools for example by EMC's Archer Governance, Risk and Compliance and/or IBM OpenPages may allow ILHIE too:

   - Transform traditional document/paper based audit process to an enterprise system
   - Maintain the library of rationalized security and privacy requirements and standards
   - Centralize authoritative repository to retain and access audit information
   - Facilitate continuous risk, remediation monitoring and report assessment results

   In closing, I would like to sincerely thank the committee for allowing me to present today on this important topic related to protecting patient data and look forward for future discussions related to securing HIEs.

***Vic Bansal**: I'm open to taking any question right now.*

***Audience Member**: I am, you know, I like the idea of the assessment and the gap analysis. I was wondering, because this seems to be one size fits all, is this a scalable approach? Because what would be for a large health insurance company versus a small clinic? It has to be scalable.*

***Vic Bansal**: It's very scalable, in fact, if you're talking about the security framework-*

***Audience Member**: Yes! 'Cause that could be- I mean what one large company does versus a physician practice may be very different.*

***Vic Bansal**: Sure. So, one of the benefits we've seen where organizations have adopted such a framework is that scalability, because you can rationalize different standards of regulation that may apply to one entity versus another. So it does provide you that scale. So, it's not a one size fits all. That's kind of the beauty about the rationalization approach. Any other questions?*

***Audience Member**: Thank you. I just have a couple of quick questions on some of the terminology that was used in your presentation. The information should be made available on a need to know bases. Is that somewhat in reference to the minimum necessary requirements under HIPAA? What are you referring to?*

***Vic Bansal**: A little bit to HIPAA as well, but I think it's more in terms of the business need for that information. So there's a requirement by a provider or by the state itself, or to the patient. There's a defined business need, that's what we mean by need to know, so minimum requirement for that information. It could be governed by applicable state laws or regulation, but I think HIPAA would be one part of that, but not necessarily all encompassing on a need to know bases.*

***Audience Member**: And then the second question is right on the second page of your testimony, right above the graph or the table. The second step you mentioned was to 'select treatment options'; I didn't understand what that meant.*

***Vic Bansal**: In the context here, 'select treatment options' once we rationalize the requirements, you figure out what is applicable. Then maybe various controls or options from a risk perspective, that's what's referred to in terms of treatment options.*

***Audience Member**: Now, not in a medical sense?*

***Vic Bansal**: Not in a medical sense. Any more questions? Thank you, Mary.*

***Mary McGinnis**: Great, thank you so much, Vic. As a word of hope to the committee, this is the last time you'll see me at the podium today. We're nearing the end. But again, in the interest of time, I did save two bits of testimony from Planned Parenthood of Illinois from Panel 6 and Panel 7, respectively. Again, for their comfort, it's just two paragraphs:*

Additional testimony from Pamela Sutherland, Vice President of Public Policy of Planned Parenthood of Illinois (PPIL).

Panel 6: Patient Choice: Current and Future Technologies

Patients should be given a unique identifier. They should also have access to their own medical records. If they believe there is an inaccuracy, they should not be allowed to unilaterally change the data. Instead, a system should be in place for the patient to contact the provider to correct the data. This will ensure that if a patient does not understand a particular test or report, they will not change something they do not understand.

Panel 7: Protecting Patient Data: Security Compliance Standards for Health Information Exchanges

As stated above, patients should be assured the utmost privacy and security, particularly when it comes to sensitive health information and minors' access to confidential care. Access to data stored in the HIE should be limited to patients and the health care professionals providing them with health care. If personal patient information is accessible to public health authorities, governmental bodies, or others, patients will not have confidence in the security and privacy of the HIE. Security and privacy standards should be consistent across all HIEs in Illinois to ensure that all patients are provided the same standards and to avoid patient confusion. In order for the HIE to be successful, patients must be willing to participate. If patients do feel that the system is secure and the information they want to be private will be kept private, they will not participate.

Thank you for the opportunity to provide comments on behalf of Planned Parenthood of Illinois. If you have any questions or need additional information, please feel free to contact Pamela Sutherland at the information in your packet.

Public Comment

Patient Choice and Consent: Operational Protocols
Patient Choice: Current and Future Technologies
Protecting Patient Data: Security Compliance Standards for Health Information Exchanges
Fostering Public Trust in Health Information Exchanges: Enforcement and Mitigation Strategies
Public Comment

Mary McGinnis: *At this time we would welcome the opportunity for public comment. I don't believe we have public comment here in Chicago. Is there public comment in Springfield?*

Springfield Participant*: No, there's not.*

Mary McGinnis*: Thank you.*

Mark Chudzinski*: Back to Dr. Nick.*

VIII. Adjourn

Dr.Nicholas Panomitros*: This meeting is adjourned. And I think we have a date scheduled for July, 27th, Friday. Thank you.*